



Texas A&M University School of Law
Texas A&M Law Scholarship

Faculty Scholarship

2005

Tempest in a Teapot or Tidal Wave - Cybersquatting Rights and Remedies Run Amok

H. Brian Holland

Texas A&M University School of Law, hbholland@law.tamu.edu

Follow this and additional works at: <https://scholarship.law.tamu.edu/facscholar>



Part of the [Law Commons](#)

Recommended Citation

H. B. Holland, *Tempest in a Teapot or Tidal Wave - Cybersquatting Rights and Remedies Run Amok*, 10 J. Tech. L. & Pol'y 301 (2005).
Available at: <https://scholarship.law.tamu.edu/facscholar/140>

This Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Texas A&M Law Scholarship. For more information, please contact aretteen@law.tamu.edu.

TEMPEST IN A TEAPOT OR TIDAL WAVE? CYBERSQUATTING RIGHTS AND REMEDIES RUN AMOK

*H. Brian Holland**

I.	INTRODUCTION	302
II.	THE DEVELOPMENT OF CYBERSQUATTING REMEDIES	304
	A. <i>Overview of the Domain Name System</i>	304
	B. <i>Cybersquatting Basics</i>	307
	C. <i>Cybersquatting Remedial Systems</i>	310
	1. Early Trademark Actions	311
	2. The Anti-Cybersquatting Consumer Protection Act ...	316
	a. Conceptions of Cybersquatting	319
	b. Bad Faith	321
	3. ICANN Arbitration and the UDRP	323
	a. Confusing Similarity	329
	b. Bad Faith	331
	c. Rights and Legitimate Interests	336
III.	SITUATING CYBERSQUATTING AMONG TRADEMARK PRINCIPLES	337
	A. <i>Toward Property: Theoretical Evolution in Trademark Law</i>	337
	B. <i>Cybersquatting as a Point of Expansion</i>	342
	1. Expansion within the Substantive Terms of the ACPA	342
	2. Expansion within the Substantive Terms of the UDRP	343

* Assistant Professor of Law, Barry University School of Law; LL.M., Columbia University School of Law, with honors; J.D., American University's Washington College of Law, *summa cum laude*. This Article is based on a presentation given as part of the Computer Law Committee of the Business Law Section's seminar, "The Cyber-Law Tool Kit: What Every Practitioner Needs to Know," at the 2005 Annual Meeting of the Florida Bar Association. I would like to express my appreciation to Robert H. Thornburg, an attorney with Allen, Dyer, Doppelt, Milbrath, & Gilchrist, P.A., who organized and invited me to participate in this event. As the title of the seminar suggests, the presentation was aimed primarily at general practitioners. Although the material has been expanded somewhat for purposes of this Article, I have attempted to keep it accessible to and useful for the originally intended audience. Thanks also to my research assistants, Alexandra Steele, Kevin Wimberly, and Sandra Woodman. Finally, as always, thanks to my endlessly patient wife, Sarah, and to my children, will.com and ella.org.

3. Systemic Expansion Beyond Substantive Terms	346
IV. BEYOND PROPERTY? LOSING TOUCH WITH LIMITING PRINCIPLES	348
A. <i>Beyond Cybersquatting Exceptionalism</i>	348
B. <i>In Derogation of Constitutional Interests and the Rule of Law</i>	350
V. CONCLUSION	351

I. INTRODUCTION

The conflict at the heart of cybersquatting is in many ways conceptual. To most of its early inhabitants, the Internet embodied a separate and distinct environment — a territory unto itself.¹ As such, it was thought the online world would stand separate from existing governmental power structures premised on the idea of territorial sovereignty.² This separateness placed online actors theoretically beyond the authority of established legal systems, whose validity appeared limited by territorial boundaries and the sovereign-subject relationships occurring in the off-line world.³ Indeed, what many envisioned was an opportunity to create a self-regulating community existing within the “territory” of the Internet and built from the ground up (an ironic phrase) on the libertarian ideal.⁴

Of course, this desire for separateness did not blind members of the virtual community to the eventuality of interaction with the off-line world. The commercial potential of the network was apparent to many, if not to established brick-and-mortar commercial interests. With this in mind, on-line actors began to buy up the most desirable “locations” in this virtual world — domain names corresponding either to popular generic or descriptive terms⁵ or to trademarks held by commercial interests under off-

1. H. Brian Holland, *The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty*, J. MARSHALL J. COMPUTER & INFO. L. (forthcoming Fall 2005) (manuscript at 4, on file with author). See also David. R. Johnson & David Post, *Law And Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

2. Holland, *supra* note 1, at 5.

3. *Id.* at 5-6.

4. *Id.* at 5-6, 8.

5. See Christie L. Branson, *Was \$7.5 Million a Good Deal for Business.com? The Difficulties of Obtaining Trademark Protection and Registration for Generic and Descriptive Domain Names*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 285, 286-87 (2001) (providing an example of the registration and sale of generic and descriptive domain names at a large profit).

line legal regimes.⁶ To these speculators, the acquisition of rights in domain names was little more than a land rush in a newly created territory, free of encumbrances, rewarding those who were the first to act by purchase of a claim of right.

Existing governmental power structures and the beneficiaries of that authority saw the Internet quite differently; as an extension of the off-line world. This network, comprised of computers and wires anchored to *terra firma*, and populated by individuals located within existing real-world borders,⁷ was, in their view, far from a new and independent territory, but rather merely another medium for communication and commerce.⁸ Thus, individuals could not ignore the rights and obligations imposed by virtue of the territorial sovereign-subject relationship simply by acting in the online environment rather than off-line.⁹ There could be no land rush, because the rights in much of that "land" had already been assigned through a system of trademark rights.

Part II of this Article describes this conflict between claims of appropriated rights in the newly created territory of the Internet and the mapping of rights conferred by existing territorially based trademark systems onto Internet space. I begin with an overview of the domain name system and the basics of cybersquatting. I then discuss the development of remedial systems intended to address the problem, from the application of existing trademark law and the weaknesses in that approach, to the Anti-Cybersquatting Consumer Protection Act (ACPA)¹⁰ and the Uniform Dispute Resolution Policy (UDRP).¹¹

Part III of this Article attempts to situate cybersquatting and its remedies among trademark principles. This links two tracks of progression. The first is the evolution of trademark principles towards property-like exclusive rights. The second uses these principles as a baseline to measure the extension of certain rights applicable in the context

6. See Ughetta Manzone, *Panavision International, L.P. v. Toeppen*, 13 BERKELEY TECH L.J. 249, 250 (1998) (describing Toeppen's strategy of registering domain names reflecting well-known trademarks).

7. See Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783, 1786, 1788-89 (2002) (describing the physical level of the Internet, comprised of material objects such as wires, computers, and wires linking computers).

8. Holland, *supra* note 1, at 6-8 (discussing primarily the arguments of Jack L. Goldsmith).

9. *Id.*

10. Pub. L. No. 106-113, 113 Stat. 1536 (codified at 15 U.S.C. § 1125(d), effective Nov. 29, 1999).

11. ICANN, Uniform Domain Name Dispute Resolution Policy [hereinafter UDRP Policy] (as adopted on Aug. 26, 1999 and approved by ICANN on Oct. 24, 1999), at <http://www.icann.org/udrp/udrp-policy-24oct99.htm> (last visited Oct. 4, 2005).

of cybersquatting. Here, I focus on the incremental modifications in the substantive terms of the ACPA, and then the more drastic changes imposed in the substantive terms of the UDRP, as effectuated by procedural and institutional biases.

In Part IV of this Article, I argue that cybersquatting remedial systems, and in particular the UDRP, have lost touch with the basic principles upon which they were constructed. I point specifically to the expansion of the UDRP beyond our understanding of “cybersquatting” and into more benign instances of domain name conflict. Connecting this to the issue of trademark protections, I argue that the expanded rights described in Part III do not make sense beyond the narrow confines of “traditional” cybersquatting. Application of the UDRP to such a broad range of cases simply cannot be justified even under the most expansive view of property-like trademark rights. Even more importantly, the bargain at the heart of the UDRP — sacrificing certain constitutional protections in favor of efficiency — raises questions of validity when applied outside the most obvious and egregious cases of bad faith and abusive domain name registration.

II. THE DEVELOPMENT OF CYBERSQUATTING REMEDIES

The purpose of this section is to lay the groundwork for my discussion of the relationship between the regulation of cybersquatting and basic trademark principles. I begin with a brief overview of the domain name system and the basics of cybersquatting. In particular, I emphasize the roles of technical structure and consumer expectation in creating the demand supporting a specific concept of value. I then describe the various remedial systems for adjudicating domain name disputes, beginning with the initial use of traditional trademark infringement and related actions, followed by the development of both statutory and contract-based actions created specifically to address cybersquatting.

A. Overview of the Domain Name System

The Internet is simply a linked network of computers geographically located all over the world.¹² In order for those individual computers to

12. See, e.g., *ACLU v. Reno*, 31 F. Supp. 2d 473, 481 (E.D. Pa. 1999) (describing the Internet as “a giant network that interconnects innumerable smaller groups of linked computer networks: a network of networks”). Apparently, finding a cohesive definition of the term “Internet” has become a cumbersome project. See, e.g., Federal Networking Council Resolution: Definition of

exchange data they must be able to find one another.¹³ To accomplish this, every computer linked to this network, whether a server or a user, is assigned an Internet protocol address (IP address) that identifies network location.¹⁴ IP addresses are numerical, consisting of four numbers (called octets) separated by periods.¹⁵ Each of the four numbers can range from 0 to 255, allowing for 4.3 billion unique combinations.¹⁶ Thus, a sample IP address might be 214.37.162.82. Server IP addresses are generally “static” in that they are assigned to that server and are the same every time the server logs on to the network.¹⁷ User IP addresses are generally “dynamic” in that a new IP address may be periodically assigned by the user’s Internet Service Provider (ISP), often changing each time the user logs on to the network.¹⁸

A “Uniform Resource Locator” (URL) is an alphanumeric expression that corresponds to a particular IP address.¹⁹ A sample URL would be <http://www.yahoo.com>. A fully qualified “domain name” is a subset of the URL, as it generally does not include the reference to the access

“Internet” 10/24/95, at http://www.nitrd.gov/fnc/Internet_res.html (last visited Oct. 4, 2005). The Internet is

the global information system that — (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Id.

13. See ICANN FAQs, at <http://www.icann.org/faq/> (last visited Oct. 4, 2005) (building on this analogy of location, and the ability to “find” a specific computer in a specific place, even when that place is “virtual,” by explaining that “[e]very computer on the Internet has a unique address — just like a telephone number”).

14. *Id.* (explaining that a computer’s network address is comprised of “a rather complicated string of numbers . . . called its ‘IP address’”).

15. Understanding IP Addressing, at <http://www.webopedia.com/DidYouKnow/Internet/2002/IPaddressing.asp> (last visited Oct. 4, 2005).

16. *Id.* IP addresses are represented in decimal rather than binary form. *Id.* “For example, the IP address 168.212.226.204 in binary form is 0101000.11010100.11100010.11001100.” *Id.* (calculations by author).

17. IP Addresses, at http://www.pcmag.com/encyclopedia_term/0,2542,t=IP+address&I=45349,00.asp (last visited on Oct. 4, 2005).

18. *Id.*

19. See URL, at <http://www.webopedia.com/TERM/U/URL.html> (last visited Oct. 4, 2005).

method (here, <http://> or hypertext transfer protocol).²⁰ The purpose of a domain name is to make Internet locations easier to remember by substituting a familiar word or string of letters for the apparently random numbers of an IP address.²¹

Each domain name contains several references. Many, but not all domain names begin with a <www> reference, indicating that they are part of the World Wide Web.²² This is followed by the second-level domain (also referred to as the “label”) and the top-level domain (also referred to as the “extension”), with each of these references separated by periods (also referred to as a “dot”).²³ Thus, in this example, if the second-level domain is <yahoo> and the top-level domain is <com>, then the domain name is <www.yahoo.com>.

The domain name system (DNS) is a mapping mechanism that correlates domain names to IP addresses.²⁴ The DNS is overseen by the Internet Corporation for Assigned Names and Numbers (ICANN).²⁵ ICANN supervises “the distribution of unique IP addresses and domain names” to “ensure that every address is unique” and “that each domain name maps to the correct IP address,” so that “all users of the Internet can find all valid addresses.”²⁶ ICANN is also responsible for accrediting domain name registrars.²⁷

20. See FQDN, at http://www.pcmag.com/encyclopedia_term/0,2542,t=fully+qualified+domain+name&I=43453,00.asp (last visited Oct. 4, 2005).

21. ICANN FAQs, *supra* note 13 (stating that “IP addresses are hard to remember” and that domain names make “using the Internet easier by allowing a familiar string of letters ... to be used instead of the arcane IP address”). See also *id.* (stating that a domain name is “a ‘mnemonic’ device that makes [IP] addresses easier to remember”).

22. See WWW, at http://www.pcmag.com/encyclopedia_term/0,2542,t=www&I=54922,00.asp (last visited Oct. 4, 2005).

23. See Internet Domain Name, at http://www.pcmag.com/encyclopedia_term/0,2542,t=second+level+domain&i=45215,00.asp (last visited Oct. 4, 2005).

24. See DNS, at http://www.pcmag.com/encyclopedia_term/0,2542,t=DNS&i=41620,00.asp (last visited Oct. 4, 2005).

25. ICANN FAQs, *supra* note 13 (stating that ICANN “is responsible for managing and coordinating the Domain Name System”).

26. *Id.* “The first point of entry for resolving a domain name” is a root server. A root server is “[o]ne of several domain name system (DNS) servers on the Internet that contain the IP addresses of the top level domain (TLD) registry organizations that maintain the global domains (.com, .net, .gov, etc.) and country code domains (.uk, .ca, .fr, etc.) . . . [T]here are currently 34 root servers throughout the world operated by government agencies and private organizations, all of which contain the same data.” Root Server, at http://www.pcmag.com/encyclopedia_term/0,2542,t=root+server&I=50620,00.asp (last visited Oct. 4, 2005).

27. ICANN FAQs, *supra* note 13.

Domain name registrars assign names on a “first-come, first-served” basis.”²⁸ Registration is maintained for an annual fee and includes priority renewal in near perpetuity.²⁹ The registrar is required to “keep records of the [registrant’s] contact information and submit [certain] technical information to a central directory known as the ‘registry.’”³⁰ However, registrars do not consider the trademark significance of (or possible infringement resulting from) a particular registration.³¹

B. Cybersquatting Basics

Cybersquatting has been defined as “the deliberate, bad-faith, and abusive registration of Internet domain names in violation of the rights of trademark owners.”³² Usually, the cybersquatter intends to profit from the sale of rights in the domain name at an inflated price.³³ A variation on this practice is typosquatting, “when a party registers a domain name that is

28. Scott D. Sanford, *Nowhere to Run . . . Nowhere to Hide: Trademark Holders Reign Supreme in Panavision Int’l, L.P. v. Toeppen*, 29 GOLDEN GATE U. L. REV. 1, 5 (1999) (describing the policies of NSI, the then-dominant registrar, as registering “domain names on a ‘first come, first served’ basis”); Manzone, *supra* note 6, at 249 (noting that the “assignment of domain names has been structured on a first-come, first-served basis”).

29. See, e.g., Network Solutions: Learn About Domain Names [hereinafter Network Solutions] (offering a “100 year domain name service . . . for domain names that you want to protect”), at <http://www.networksolutions.com/learning-center/domain-name-registrations.jhtml> (last visited Oct. 4, 2005).

30. ICANN FAQs, *supra* note 13.

31. Victoria Holstein-Childress, *Lex Cyberus: The UDRP as a Gatekeeper to Judicial Resolution of Competing Rights to Domain Names*, 109 PENN ST. L. REV. 565, 567 (2004):

Further intensifying the competition between these groups for use of particular domain names is a lack of any effective regulatory control over domain name registration; domain names are assigned primarily on a first-come first-served basis by non-governmental bodies without any inquiry into potential conflicts between the requested domain name and registered trademarks.

See also Philip G. Hampton, II & Jennifer M. McCue, *Internet Corporation for Assigned Names and Numbers / Anticybersquatting Consumer Protection Act of 1999: Dealing with Cyber-Claims*, SK102 A.L.I.-A.B.A. 13, 16 (2005) (stating that “Domain names are assigned without reference to whom may be ‘entitled’ to it” and that “the domain name registrars are not required to confirm that a particular registrant of a domain name has the trademark rights associated with that particular domain name”).

32. S. REP. NO. 106-140, at 4 (1999).

33. See, e.g., Cybersquatting, NetLingo.com Dictionary (stating in its definition of cybersquatting that the “intent [of a cybersquatter] is not to develop it into a Web site but rather to sell it to the rightful owner for a big profit”), at <http://www.netlingo.com/lookup.cfm?term=cybersquatting> (last visited Oct. 4, 2005).

very close to another's trademark or name for the purpose of capitalizing on an Internet user's typographical errors when entering a web address."³⁴ This variation falls into the larger category of cybersquatting for the purpose of traffic diversion, in which the cybersquatter registers a misspelling, pluralization, or other obvious derivation of another's mark in order to divert traffic to some web site other than the one sought by the consumer.³⁵ Other variations include cyberjesters and cyberzealots, parties attempting to make humorous or political statements about the trademark holder, and cyberpornographers (more broadly known as cyberopportunists), parties seeking to capitalize on the goodwill of the trademark holder to steer Internet users to pornographic web sites.³⁶

In economic terms, the development of cybersquatting was nearly inevitable and remarkably simple. In order to map correctly to an IP address, a domain name must be unique.³⁷ As a result, domain names are, by definition, exceptionally scarce.³⁸ However, in the early days of the Internet, there was little demand for domain names. As such, the rights in a domain name could be easily and inexpensively acquired and held (or warehoused) almost indefinitely,³⁹ in expectation of future demand. Eventually demand did develop primarily along two lines, both of which are linked to consumer expectations. The first was the rapid development of online commerce, both in terms of actual sales and mere presence. This produced an expectation among consumers that any business of significant size could be found online. The second was the development of a process for navigating the Internet that placed a premium on consumer expectations as to what domain name addresses would lead them to a particular business. These are explored in turn.

The first influence on the demand for domain names was the rapid development of online commerce. Although the collection of official statistics has suffered somewhat from the application of uneven measurement standards, U.S. Census Bureau figures provide some estimation as to the growth of e-commerce. According to the annual "E-Stats" report, in 1999 e-commerce transactions totaled approximately \$659 billion of which \$15 billion was in the form of business-to-consumer retail

34. Leonard D. DuBoff & Christy O. King, *Cyber Troubles: Resolving Domain Name Disputes*, 65-MAY OR. ST. B. BULL. 33, 33 (May 2005).

35. See *infra* Part II(C)(2)(a) (quoting S. REP. NO. 106-140; describing various forms of cybersquatting).

36. *Id.*

37. See ICANN FAQs, *supra* note 13.

38. See Holstein-Childress, *supra* note 31, at 567 (noting that "a domain name is both global and unique").

39. See, e.g., Network Solutions, *supra* note 29.

sales.⁴⁰ Just four years later, in 2003, e-commerce transactions had grown to approximately \$1.7 trillion, with business-to-consumer retail sales accounting for \$106 billion of that total.⁴¹ These statistics certainly provide some measure of consumer expectation, but they do not tell the entire story. Consumers quickly came to expect some sort of Internet presence, even without the ability to consummate on-line transactions. Thus, while only 34% of the Fortune 500 companies had web sites in 1996, that number had grown to 80% by 1997.⁴² Just 2 years later, in 1999, nearly every one of the top one hundred Fortune 500 companies had a corporate web site.⁴³

The second influence on the increased demand for domain names was the development of a process of online navigation largely driven by consumer expectation, coupled with intuition, situational biases, and cumulative trial and error. This approach has been encouraged by minimal search costs, increasingly more accurate results, and the perceived lack of more efficient alternatives.⁴⁴ For example, if a user is looking for a traditional, well-known off-line company on the Internet, most users simply take a stab at it, guessing that Microsoft software can be found at <microsoft.com> and that Target department stores can be found at <target.com>.⁴⁵ In those instances they would be right on both counts. But what if the user turns out to be wrong? Frustration in failing to quickly find

40. See United States Department of Commerce: 1999 E-Stats (Mar. 7, 2001), available at <http://www.census.gov/eos/www/papers/1999/1999estatstext.pdf> (last visited Nov. 14, 2005).

41. See United States Department of Commerce: 2003 E-Stats (May 11, 2005), available at <http://www.census.gov/eos/www/papers/2003/2003finaltext.pdf> (last visited Nov. 14, 2005).

42. Erin M. Davis, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 ALB. L.J. SCI. & TECH. 683, 687 (2002).

43. Erick D. Prohs, *Periodic Financial Report — A Relic of the Past?*, 27 J. CORP. L. 481, 489 n.63 (2002).

44. This may be changing as search methods become more accurate and discerning, and more efficiently embedded in the user interface. See, e.g., John Battelle, *The Birth of Google*, WIRED, Aug. 2005 (describing the basic theory of Google's search method), available at http://www.wired.com/wired/archive/13.08/battelle_pr.html (last visited Oct. 4, 2005).

45. Holstein-Childress, *supra* note 31, at 567 (positing that "Internet users tend to intuit web addresses of the companies they seek by merely entering the corporate name followed by a generic top level domain (gTLD) such as <.com>"); *id.* at 570 (observing that "A domain name that incorporates a particular mark facilitates the ability of the intuitive Internet browsing individual to locate a web site devoted to the trademark holder's enterprise"); *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1044-45 (9th Cir. 1999) (describing a process of navigation in which "Oftentimes, an Internet user will begin by hazarding a guess at the domain name, especially if there is an obvious domain name to try. Web users often assume, as a rule of thumb, that the domain name of a particular company will be the company name followed by '.com.'").

the correct web site can easily result in diversion.⁴⁶ For instance, if I am flying from Orlando to San Francisco I might first try <www.northwest.com>, but I will not find Northwest Airlines, as I might expect.⁴⁷ Instead, I will find myself at a travel web site promoting Oregon, Washington, and British Columbia, with no sign of Northwest Airlines.⁴⁸ But if I choose <www.southwest.com>, I head straight to Southwest Airlines and will likely buy my ticket there.⁴⁹ In the absence of actual knowledge, consumer expectations — incorporating knowledge derived from the off-line world, intuition, situational biases, etc. — will continue to drive online navigation. If a business is not located where I expect it to be, I may well go elsewhere.⁵⁰

In the mid- to late-1990s, certain individuals foresaw the commercial potential of the Internet, the tendency towards expectation-driven navigation, and the value that such expectation created in domain names that are exceptionally scarce. Joe Toeppen was one of those individuals.⁵¹ Early on, Toeppen registered hundreds of domain names, many of which were trademarks.⁵² He then offered to sell them to the highest bidder, regardless of whether that person was the trademark holder or its chief rival.⁵³ This upset many trademark holders, and made Joe Toeppen the poster child for cybersquatting. The question for trademark holders was how to gain control of these domain names by (a) utilizing existing laws and (b) seeking the passage of new or revised laws or contract-based regulations.

C. Cybersquatting Remedial Systems

In the mid-1990s, there was no law that specifically prohibited or imposed liability for cybersquatting. Accordingly, when the practice first appeared, attorneys were forced to cast about to find some existing legal principle that could put an end to the practice. Trademark law seemed the

46. See Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 HOUS. L. REV. 777, 780-81 (2004) (discussing the role of mistake, diversion, and frustration in on-line trademark disputes).

47. See Northwest.com, at <http://www.northwest.com/> (last visited Oct. 4, 2005) (linking to a travel-oriented web site claiming the title of “gateway to the beautiful Pacific Northwest”). See also Holstein-Childress, *supra* note 31.

48. Northwest.com, *supra* note 47.

49. See Southwest Airlines, at <http://www.southwest.com/> (last visited Oct. 4, 2005).

50. See Dogan & Lemley, *supra* note 46.

51. Manzone, *supra* note 6, at 250-51 (describing Toeppen’s cyber-speculating activities).

52. *Id.*

53. *Id.*

logical choice, and indeed it was the most successful. However, it was not ideal.⁵⁴ In this section, I provide an overview of early attempts to utilize traditional trademark infringement and dilution actions to combat cybersquatting. I then discuss the development of two coexistent remedial devices aimed specifically at cybersquatters, the Anti-Cybersquatting Consumer Protection Act and the Uniform Domain Name Dispute Resolution Policy.

1. Early Trademark Actions

The first attempts to dislodge cybersquatters utilized traditional trademark and related actions: direct trademark infringement and unfair competition, dilution, and secondary liability (contributory infringement and vicarious liability).⁵⁵ However, the fit between these established actions and the “wrong” of cybersquatting was not particularly comfortable and the corresponding results for trademark holders, although not entirely unsuccessful, were nevertheless disappointing.⁵⁶ Indeed, these lackluster results ultimately led to the establishment of alternate regulatory regimes specifically applicable to cybersquatting. However, the principles established in these early cases remain pertinent to the resolution of other domain name disputes. A brief overview of these initial actions is therefore helpful in any evaluation of remedial alternatives in other types of domain name disputes.

Direct infringement under section 32 of the Lanham Act requires proof of (a) ownership of the mark, (b) use of the mark in (interstate) commerce, and (c) likelihood of confusion between the mark and the defendant’s allegedly infringing use.⁵⁷ An allegation of unfair competition under section 43(a) of the Lanham Act⁵⁸ will usually accompany a section 32 claim but will also fail if the section 32 claim is unsuccessful.⁵⁹ In the

54. See Hampton & McCue, *supra* note 31, at 17 (stating that “Classic trademark theories, such as infringement and dilution, are largely ineffective in preventing cybersquatting.”).

55. See generally Jennifer Golinveaux, *What’s in a Domain Name? Is “Cybersquatting” Trademark Dilution?*, 33 U.S.F. L. REV. 641, 654-55 (1999) (providing a relatively early, but post-FTDA look at efforts to pursue cybersquatters under existing trademark actions).

56. *Id.* at 657.

57. 15 U.S.C. § 1114 (2005). See, e.g., Checkpoint Systems, Inc. v. Check Point Software Tech., Inc., 269 F.3d 270, 279 (3d Cir. 2001); *Jews for Jesus v. Brodsky*, 993 F. Supp. 282, 294 (D. N.J. 1998).

58. 15 U.S.C. § 1125(a) (1999).

59. This linkage arises from a common and elemental foundation. See J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 23:1 (4th ed. 1996) (noting that “While issues of priority, secondary meaning, assignment, and the like, may be present in some cases, the test of likelihood of confusion is the touchstone of trademark infringement as well as

context of cybersquatting, the “use” requirement poses the greatest hurdle to a successful direct infringement claim.

The use requirement encompasses two distinct elements.⁶⁰ The first is jurisdictional, addressing Congress’s power to legislate matters affecting interstate commerce — the constitutional authority invoked as the premise for federal regulation of trademarks.⁶¹ The second is a matter of substantive law, as sections 32 and 43(a) of the Lanham Act expressly require “use in commerce” by the defendant as an element of direct infringement.⁶² Both aspects of the use requirement can be very difficult to establish in a cybersquatting case.

Courts have ruled that the creation and maintenance of an Internet web site satisfies the jurisdictional use requirement, because the network over which that web site is made available utilizes interstate phone lines and similar technologies.⁶³ However, merely registering and warehousing a domain name without establishing a related Internet web site does not satisfy the jurisdictional use requirement.⁶⁴ This raises difficult issues for the trademark holder, because for most cybersquatting purposes no web site is required.⁶⁵ It is the registrant/cybersquatter’s rights in the domain name, and his ability to transfer those rights, that make cybersquatting profitable, not the existence of a corresponding web site.⁶⁶

The substantive use requirement can also pose problems in cybersquatting cases. A direct infringement claim requires use in

unfair competition”). *But see* David J. Kera & Theodore H. Davis, Jr., *United States: The Fifty-Fifth Year of Administration of the Lanham Trademark Act of 1946*, 93 TRADEMARK REP. 197, 365 (2003) (discussing two recent cases that present “useful reminders that a finding of unfair competition can lie even if accompanying claims for infringement fail.”).

60. *See, e.g.*, *Intermatic, Inc. v. Toeppen*, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996) (an early case of cybersquatting, suggesting the two aspects of use in commerce).

61. *See, e.g.*, *Planned Parenthood Fed’n of Am., Inc. v. Bucci*, 42 U.S.P.Q.2d 1430, 1434 (S.D.N.Y. 1997) (stating that “The ‘use in commerce’ requirement of the Lanham Act is a jurisdictional predicate to any law passed by Congress”).

62. 15 U.S.C. §§ 1114(1)(a) (2005), 1125(a)(1) (1999).

63. *Bucci*, 42 U.S.P.Q.2d at 1434 (indicating that the jurisdictional use requirement is met, in part, because Internet users “must use interstate telephone lines to access [a] web site on the Internet”). *See also* *Steele v. Bulova Watch Co.*, 344 U.S. 280, 283 (1952) (stating that “The Lanham Act . . . confers broad jurisdictional powers upon the courts of the United States,” thus effectuating the statutory “intent . . . to regulate commerce within the control of Congress”) (internal quotations omitted).

64. *See generally* *Jews for Jesus v. Brodsky*, 993 F. Supp. 282, 307 (D. N.J. 1998) (finding that the “mere registration of a domain name, without more, is not a ‘commercial use’ of a trademark”).

65. *See infra* Part II(C)(2)(a) (quoting S. REP. NO. 106-140) (describing various forms of cybersquatting, several of which do not require a web site).

66. *Id.*

commerce as a trademark; that is, "in connection with . . . the sale, . . . distribution, or advertisement of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive."⁶⁷ A domain name may, depending upon its function, constitute either actionable trademark use or non-infringing, non-trademark use. The distinction here is between the domain name's technical function as an indication of network location and its potential to function as an identifier of the source of goods or services.⁶⁸ Direct infringement requires that the domain name serve the latter function⁶⁹ and that such use is likely to confuse.⁷⁰ Therefore, where no web site is established, trademark use is absent.⁷¹ Likewise, where a web site is entirely unrelated to the sale, distribution, or advertisement of goods or services, trademark infringement can usually not be found, although, some courts will cast an extremely wide net to find such a relationship.⁷²

However, even if a trademark holder pursuing a cybersquatter is able to satisfy the use requirements, she may well run into additional difficulties in proving likelihood of confusion, albeit to a lesser extent. One of the most troublesome factors⁷³ for trademark holders tends to be

67. 15 U.S.C. § 1114(1)(a).

68. See *Lockheed Martin Corp. v. Network Solutions, Inc.* 985 F. Supp. 949, 956 (C.D. Cal. 1997), *aff'd* by 194 F.3d 980 (9th Cir. 1999) (observing that "Domain names present a special problem under the Lanham Act because they are used for both a non-trademark technical purpose, to designate a set of computers on the Internet, and for trademark purposes, to identify an Internet user who offers goods or services on the Internet.").

69. See generally 15 U.S.C. § 1127 (2000) (defining a "trademark" as a "word, name, symbol, or device" used, *inter alia*, "to indicate the source of the goods").

70. 15 U.S.C. §§ 1114(1)(a), 1125(a)(1)(A) (1999).

71. See generally *Lockheed Martin*, 985 F. Supp. at 957 (indicating that the act of registration is not itself trademark use).

72. See *id.* at 956 (stating that "Domain names, like trade names, do not act as trademarks when they are used merely to identify a business entity; in order to infringe they must be used to identify the source of goods or services."). See also *id.* at 957 (citing *Lucasfilm, Ltd. v. High Frontier*, 622 F. Supp. 931, 933 (D.D.C. 1985), for the proposition "that property rights in a trademark do not extend to the use of the trademark to express ideas unconnected with the sale or offer for sale of goods or services"); *Hampton & McCue*, *supra* note 31, at 17 (stating that the Lanham Act "requires use or an intention to use the infringed mark in commerce and [that] several courts have held that the infringer must be using the mark on goods or services that would be confused with the goods or services upon which the registrant is using the mark").

73. The likelihood-of-confusion analysis is generally undertaken by weighing various factors. See, e.g., *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961). The eight *Polaroid* factors are: (1) strength of the trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user may "bridge the gap" by developing a product for sale in the market of the alleged infringer's product; (5) evidence of actual consumer confusion; (6) evidence that the imitative mark was adopted in bad

similarity of the goods and competitive proximity.⁷⁴ In analyzing this factor, many courts consider the web sites themselves to be the good in question, rather than the products or services offered on the web site.⁷⁵ Thus, the court will examine the defendant's web site and the plaintiff's web site (perhaps speculating what the plaintiff's web site would look like if it is not yet in existence) to determine similarity.⁷⁶ Where a cybersquatter's web site is largely unrelated to the business of the trademark holder, this will weigh against a finding of likelihood of confusion.⁷⁷ However, with the advent of the initial-interest-confusion doctrine, the content of the web site tends to take a back seat to the similarity between the mark and the domain name, particularly if they are identical.⁷⁸

Actions under the federal dilution statute, found in § 43(c) of the Lanham Act, have been more successful in cybersquatting cases, although the trademark holder may encounter some of the same difficulties present in direct infringement actions.⁷⁹ The primary benefit of a dilution action is that, unlike direct infringement, it does not require the plaintiff to show likelihood of confusion or competition between the parties as does direct

faith; (7) respective quality of the products; and (8) sophistication of consumers in the relevant market. *Id.* See also *AMF, Inc. v. Sleekcraft Boats*, 599 F.2d 341 (9th Cir. 1979).

74. Outside of the Internet context, this factor implicates two related inquiries. The first looks at the products themselves. The second looks at the markets and channels of trade in which those products appear. The larger inquiry blends elements. On the Internet, as applied to domain names, it is difficult, if not impossible, to cut the question so finely. Is the good, the domain name, the web site, the content of the web site, or the products sold there? Is the market defined by potential customers for the product you define or all Internet users who might navigate to that particular domain name?

75. See, e.g., *Intermatic, Inc. v. Toeppen*, 947 F. Supp. 1227, 1235 (N.D. Ill. 1996).

76. *Id.*

77. See generally *AMF, Inc.*, 599 F.2d at 351 (observing that similarity of trademarks are "tested on three levels: sight, sound and meaning").

78. See, e.g., *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066 (9th Cir. 1999).

79. The issue of "use" is particularly troublesome:

[T]he mere act of registering the domain name, without any actual use of the domain name in a web site or e-mail address, and without an offer to sell the address, may not be enough to trigger the anti-dilution statutes. Simply registering the name is probably not "commercial use" of the domain name.

Hampton & McCue, *supra* note 31, at 17.

infringement.⁸⁰ Instead, it is enough to show that the defendant's use lessens "the capacity of a famous mark to identify and distinguish goods or services."⁸¹ However, this apparently lower standard does not make dilution entirely successful against cybersquatters. First, dilution is only applicable to a select group of marks, those that are "famous" and "distinctive."⁸² Second, the U.S. Supreme Court has recently held that § 43(c) requires proof of actual dilution,⁸³ although this was generally not required during the height of the cybersquatting problem. Third, as with a direct infringement action under §§ 32 and 43(a) of the Lanham Act, a dilution action still requires that the trademark holder prove use in commerce as a trademark,⁸⁴ raising the difficulties discussed above.⁸⁵ Finally, the dilution statute requires that the defendant's use be "commercial,"⁸⁶ and interpretation of this requirement has been somewhat uneven.

The final obstacle facing trademark holders in the pursuit of cybersquatters is the problem of personal jurisdiction.⁸⁷ Many cybersquatters reside abroad.⁸⁸ Their only contact with the United States is that they own rights to a domain name that under the law of the United States allegedly infringes the trademark of another.⁸⁹ In such instances, it becomes extremely difficult to establish the minimum contacts required to

80. *Moseley v. V Secret Catalogue, Inc.*, 537 U.S. 418, 429 (2003) (noting that "Neither the absence of any likelihood of confusion nor the absence of competition, however, provides a defense to [a] statutory dilution claim").

81. *Id.* at 433; *see generally* 15 U.S.C. § 1127 (2000).

82. 15 U.S.C. § 1125(c)(1) (2005) (providing a non-exhaustive list of factors to be considered in determining whether a mark is distinctive and famous for the purposes of dilution).

83. *Cf. Moseley*, 537 U.S. at 433, *with Hampton & McCue*, *supra* note 31, at 17 (stating that "in light of the recent Supreme Court pronouncement that to prevail under the [federal dilution statute], a party must prove actual dilution, it is even less likely that cybersquatting can be successfully stopped under that act").

84. 15 U.S.C. § 1125(c)(1).

85. *See supra* Part II(C)(1).

86. 15 U.S.C. § 1125(c)(1).

87. *See* Andrew J. Grotto, *Due Process and In Rem Jurisdiction Under the Anti-Cybersquatting Consumer Protection Act*, 2 COLUM. SCI. & TECH. L. REV. 1, 5-6 (2001) (describing the jurisdictional issues preceding and motivating, in part, the passage of the ACPA, including the rejection of *in rem* jurisdiction in existing trademark actions).

88. *See id.* at 6-9 (discussing domain name registration as sufficing for minimum contracts with forum jurisdiction). *See also* Jinku Hwang, *Is the ACPA a Safe Haven for Trademark Infringers? – Rethinking the Unilateral Application of the Lanham Act*, 22 J. MARSHALL J. COMPUTER & INFO. L. 655, 655-56 (2004) (describing the issue of cybersquatters residing abroad).

89. Hwang, *supra* note 88, at 655.

gain personal jurisdiction over the cybersquatter.⁹⁰ Furthermore, *in rem* jurisdiction has been found impermissible in actions under §§ 32, 43(a), and 43(c).⁹¹ Additionally, some cybersquatters actively seek to obscure their identity, making them impossible or extremely expensive to pursue.⁹² This hurdle has often proven insurmountable.

Not surprisingly, having failed in many cases to gain redress from the cybersquatters, trademark holders sought relief from the domain name registrars.⁹³ A full discussion of these efforts is not pertinent to this Article. It is enough to say that actions against registrars based on various theories of vicarious liability, as well as those based in tortious interference with business relationships, were unsuccessful.⁹⁴

2. The Anti-Cybersquatting Consumer Protection Act

In response to trademark holder concerns, the Anti-Cybersquatting Consumer Protection Act (ACPA) was enacted in the fall of 1999.⁹⁵ The ACPA added § 43(d) to the Lanham Act to expressly provide a civil remedy against cybersquatting,⁹⁶ and in doing so addressed many of the issues discussed previously. In passing the ACPA, Congress leveraged the modicum of success trademark holders had achieved using the dilution

90. See Grotto, *supra* note 87, at 6-9 (describing "The Jurisdictional Quagmire" implicated by domain name disputes, particularly in the case of foreign defendants).

91. See *id.* at 7-8 (discussing, *inter alia*, the decision in *Porsche Cars of N. Am., Inc. v. Porsche.com*, 51 F. Supp. 2d 707 (E.D. Va. 1999), *rev'd on other grounds*, *Porsche Cars of N. Am., Inc. v. AllPorsche.com*, 215 F.3d 1320 (4th Cir. 2000)).

92. S. REP. NO. 106-140, at 9 (1999) (noting in the Senate Judiciary Committee's Report on the ACPA that a "significant problem faced by trademark owners in the fight against cybersquatting is the fact that many cybersquatters register domain names under aliases or otherwise provide false information in their registration applications in order to avoid identification and service of process by the mark owner").

93. See, e.g., *Lockheed Martin Corp. v. Network Solutions, Inc.*, 141 F. Supp. 2d 648, 656 (N.D. Tex. 2001) (rejecting a claim under the Texas state anti-dilution statute, primarily because registration of a domain name does not constitute either use of a mark or intent to profit from the mark).

94. See *id.* at 655-56.

95. Pub. L. No. 106-113, 113 Stat. 1536 (codified at 15 U.S.C. § 1125(d), effective Nov. 29, 1999).

96. S. REP. NO. 106-140, at 2 (1999) (finding that "[a]mendments to the Trademark Act of 1946 would clarify the rights of a trademark owner to provide for adequate remedies and to deter cyberpiracy and cybersquatting").

statute against cybersquatters, but made some important changes to make it easier for trademark holders to prevail.⁹⁷

The ACPA requires a showing that the defendant, with bad intent to profit, registered, trafficked in, or used a domain name that (a) if a mark is distinctive, is identical or confusingly similar to that mark, or (b) if the mark is famous, is identical or confusingly similar to or dilutive of that mark.⁹⁸ The ACPA applies equally to registered and unregistered marks and without regard to the goods or services of the parties.⁹⁹ The statute includes a non-exclusive list of nine factors to be considered in the determination of "bad faith intent,"¹⁰⁰ but provides a safe harbor upon a showing that the defendant believed and had reasonable grounds to believe that the use of the domain name was fair use or otherwise lawful.¹⁰¹ Remedies available under the ACPA include an order compelling the forfeiture or transfer of a domain name or cancellation of the registration,¹⁰² statutory damages between \$1,000 and \$100,000 per domain name (in lieu of actual damages or profits);¹⁰³ and injunctive relief and damages as otherwise available under the Lanham Act.¹⁰⁴ The ACPA also provides a solution to the problem of jurisdiction.¹⁰⁵ If a trademark holder cannot get personal jurisdiction over, or cannot with due diligence find, the registrant, then the statute provides for *in rem* jurisdiction over the domain name itself.¹⁰⁶ However, in such cases, remedies are statutorily

97. See Hampton & McCue, *supra* note 31, at 26 (stating that "the ACPA eliminates many substantive and jurisdictional problems that trademark owners were facing in trying to adapt trademark law to the cybersquatting situation").

98. 15 U.S.C. § 1125(d)(1)(A).

99. *Id.*

100. *Id.* § 1125(d)(1)(B)(i).

101. *Id.* § 1125(d)(1)(B)(ii). This safe harbor has, however, often been stringently applied. See Hampton & McCue, *supra* note 31, at 28 (citing *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 369 (4th Cir. 2001), for the proposition that "a defendant who acts even partially in bad faith cannot benefit from the safe harbor provisions of the ACPA").

102. 15 U.S.C. § 1125(d)(1)(C).

103. 15 U.S.C. § 1117(d) (2004).

104. *Id.*

105. See Hwang, *supra* note 88, at 656 (stating that the *in rem* provisions of the ACPA "made all the debates on personal jurisdiction useless").

106. 15 U.S.C. § 1125(d)(2); see also Hampton & McCue, *supra* note 31, at 28 (stating that in enacting the ACPA "Congress . . . attempted to alleviate one of the main difficulties in bringing suit against a cybersquatter, obtaining personal jurisdiction, by providing for *in rem* jurisdiction").

A trademark owner may pursue this option in two scenarios: (1) if the registrant is not subject to personal jurisdiction in the forum, such as when the cybersquatter is located in a foreign country; or (2) when the trademark owner cannot locate the registrant through due diligence, such as when incomplete or inaccurate

limited to an order compelling the forfeiture or transfer of the domain name or cancellation of the registration.¹⁰⁷

Substantively, the ACPA differs from direct infringement and dilution actions in at least six important ways. First, the ACPA broadens the definition of cybersquatting beyond that developed in prior case law.¹⁰⁸ Second, the ACPA eliminates the use-in-commerce requirement applicable to both direct infringement and dilution actions.¹⁰⁹ Third, the ACPA omits the commercial-use requirement found in the federal dilution statute.¹¹⁰ Fourth, the ACPA establishes bad faith as a necessary element of liability,¹¹¹ rather than just one factor among many, and focuses the bad faith inquiry (in accord with these first three distinctions) on the broad notion of the registrant's intent to profit through the mere registration, trafficking, or use of a domain name.¹¹² Fifth, the ACPA asks whether a domain name is "identical or confusingly similar" to the plaintiff's mark¹¹³ and not whether the parties' domain names are likely to be confused.¹¹⁴

information was provided to the registrar. However, a plaintiff cannot proceed under both *in rem* and *in personam* jurisdiction, since it is not possible to prove *in personam* jurisdiction while also proving its absence for *in rem* jurisdiction.

Id. at 28-29 (citations omitted). *See also* Hwang, *supra* note 88, at 657-58 (noting that "*in rem* and *in personam* jurisdiction are mutually exclusive in the ACPA," and that "the mark owner [asserting an action *in rem*] must bear the burden of demonstrating the absence of *in personam* jurisdiction over an alleged infringer"). Proceedings *in rem* must generally be filed in the judicial district in which the domain name registrar or registry is located:

[P]laintiffs seeking to bring an *in rem* action against a domain name owner must bring the case in the domain name registrar's judicial district, and cannot just bring the action in any district they want. However, an *in rem* action does not require minimum contacts by the domain registrant, only that the registrar be located in the judicial district.

Hampton & McCue, *supra* note 31, at 29 (citations omitted). *See also* Hwang, *supra* note 88, at 658 (reporting that "Courts have held that *in rem* jurisdiction lies only in the judicial district where the registrar, registry, or other authority is located as specified in § 1125(d)(2)(A)").

107. 15 U.S.C. § 1125(d)(2)(D)(I).

108. *See infra* Part II(C)(2)(a).

109. *See generally* 15 U.S.C. § 1125(d); *see also* S. REP. NO. 106-140, at 9 (1999).

110. *See generally* 15 U.S.C. § 1125(d); *see also* S. REP. NO. 106-140, at 9.

111. 15 U.S.C. § 1125(d)(1)(A)(i).

112. *Id.* § 1125(d)(1)(B)(i)(V) - (VIII).

113. *Id.* § 1125(d)(1)(A)(ii).

114. The Eighth Circuit has, as Hampton and McCue note, recently addressed this distinction:

That the domain name be confusingly similar to the mark is another requirement of the ACPA. In *Coca-Cola Co. v. Purdy*, 382 F.3d 774 (8th Cir. 2004), the

Sixth, unlike the federal dilution statute, which applies only to marks that are both famous *and* distinctive, the ACPA applies to marks that are either famous *or* distinctive¹¹⁵ (whether such distinctiveness is inherent or acquired through use). However, the ACPA provides broader protection for famous marks than it does for non-famous but distinctive marks.¹¹⁶ Two of these distinctions — the broadening of the definition of cybersquatting and the emphasis on a registrant's bad faith intent to profit — warrant additional comment.

a. Conceptions of Cybersquatting

Congress made clear that the ACPA was intended to apply to at least four conceptions of cybersquatting, including those situations in which someone other than the trademark holder registers a domain name:

[1] Some register well-known brand names as Internet domain names in order to extract payment from the rightful owners of the marks, who find their trademarks "locked up" and are forced to pay for the right to engage in electronic commerce under their own brand name.¹¹⁷ [2] Others register well-known marks as domain

District Court upheld a preliminary injunction against Purdy prohibiting him from using domain names confusingly similar to plaintiff's. The court stated that the question under the ACPA is not whether the domain names are likely to be confused with a plaintiff's domain name, but whether they are identical or confusingly similar to a plaintiff's mark. It is the challenged domain name and the plaintiff's mark which are to be compared. The inquiry under the ACPA is thus narrower than the traditional multifactor likelihood of confusion test for trademark infringement. The fact that confusion about a website's source or sponsorship could be resolved by visiting the website is not relevant to whether the domain name itself is identical or confusingly similar to a plaintiff's mark.

Hampton & McCue, *supra* note 31, at 30.

115. 15 U.S.C. § 1125(d)(1)(A)(ii).

116. *Compare id.* § 1125(d)(1)(A)(ii)(I), with *id.* § 1125(d)(1)(A)(ii)(II).

117. S. REP. NO. 106-140, at 9 (1999). The Senate Report cited the following example:

[S]everal years ago a small Canadian company with a single shareholder and a couple of dozen domain names demanded that Umbro International, Inc., which markets and distributes soccer equipment, pay \$50,000 to its sole shareholder, \$50,000 to an Internet charity, and provide a free lifetime supply of soccer equipment in order for it to relinquish the "umbro.com" name. The Committee also heard testimony that Warner Bros. was reportedly asked to pay \$350,000 for the rights to the names "warner-records.com", "warner-bros-records.com",

names and warehouse those marks with the hope of selling them to the highest bidder, whether it be the trademark owner or someone else.¹¹⁸ [3] In addition, cybersquatters often register well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's site to the cybersquatter's own site, many of which are pornography sites that derive advertising revenue based on the number of visits, or "hits," the site receives.¹¹⁹ [4] Finally, and most importantly,

"warner-pictures.com", "warner-bros-pictures", and "warnerpictures.com". *Id.* (footnotes omitted).

118. *Id.* The Senate Report cited the following example:

[T]he Committee heard testimony regarding an Australian company operating on the Internet under the name "The Best Domains," which was offering such domain names as "911porsche.com," at asking prices of up to \$60,911, with a caption that reads "PORSCHE: DO I NEED TO SAY ANYTHING?" The Committee also heard testimony regarding a similarly enterprising cybersquatter whose partial inventory of domain names — the listing of which was limited by the fact that Network Solutions will only display the first 50 records of a given registrant — includes names such as Coca-Cola, Pepsi, Burger King, KFC, McDonalds, Subway, Taco Bell, Wendy's, BMW, Chrysler, Dodge, General Motors, Honda, Hyundai, Jaguar, Mazda, Mercedes, Nissan, Porsche, Rolls-Royce, Saab, Saturn, Toyota, and Volvo, all of which are available to the highest bidder through an online offer sheet.

Id. (footnotes omitted).

119. *Id.* The Senate Report cited the following example:

[T]he Committee was informed of a parent whose child mistakenly typed in the domain name for "dosney.com," expecting to access the family-oriented content of the Walt Disney home page, only to end up staring at a screen of hardcore pornography because a cybersquatter had registered that domain name in anticipation that consumers would make that exact mistake. Other instances of diverting unsuspecting consumers to pornographic web sites involve malicious attempts to tarnish a trademark owner's mark or to extort money from the trademark owner, such as the case where a cybersquatter placed pornographic images of celebrities on a site under the name "pentium3.com" and announced that it would sell the domain name to the highest bidder. Others attempt to divert unsuspecting consumers to their sites in order to engage in unfair competition. For example, the business operating under the domain name "disneytransportation.com" greets online consumers at its site with a picture of Mickey Mouse and offers shuttle services in the Orlando area and reservations at Disney hotels, although the company is in no way affiliated with the Walt Disney Company and such fact is not clearly indicated on the site. Similarly, the domain name address "wwwcarpoint.com," without a period following "www", was used by a

cybersquatters target distinctive marks to defraud consumers, including to engage in counterfeiting activities.¹²⁰

The first and second of these conceptions essentially involve arbitrage or blackmail (depending upon your point of view) of the trademark owner, although these do not strictly implicate common notions of trademark infringement. The third conception appears to encompass two distinct principles, depending upon the identity of the registrant. One is firmly embedded in the foundations of trademark law. The other lurks in the shadows, as a manifestation of expansive trademark protections. If the registrant is a competitor of the trademark holder, then an act of cybersquatting may constitute classic diversion of trade. If the registrant is not a competitor of the trademark holder, then it looks more like an attempt to leverage the goodwill of a well-known brand. The fourth conception is simply the bait-and-switch of counterfeit goods.

b. Bad Faith

As to the ACPA's emphasis on a registrant's bad faith intent to profit, the statute provides a list of nine non-exhaustive factors to be considered in making this determination.¹²¹ The first four of these factors speak to evidence demonstrating an *absence* of bad faith:

cybersquatter to offer a competing service to Microsoft's popular Carpoint car buying service.

Id. (footnotes omitted).

120. *Id.* at 9. The Senate Report cited the following example:

[T]he Committee heard testimony regarding a cybersquatter who registered the domain names "attphonecard.com" and "attcallingcard.com" and used those names to establish sites purporting to sell calling cards and soliciting personally identifying information, including credit card numbers. We also heard the account of a cybersquatter purporting to sell Dell Computer products under the name "dellspares.com", when in fact Dell does not authorize online resellers to market its products, and a similar account of someone using the name "levis501warehouse.com" to sell Levis jeans despite the fact that Levis is the only authorized online reseller of its jeans. Of even greater concern was the example of an online drug store selling pharmaceuticals under the name "propeciasales.com" without any way for online consumers to tell whether what they are buying is a legitimate product, a placebo, or a dangerous counterfeit.

Id. (footnotes omitted).

121. 15 U.S.C. § 1125(d)(1)(B)(i).

- (I) the trademark or other intellectual property rights of the person, if any, in the domain name;
- (II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
- (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
- (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name¹²²

The next four factors, on the other hand, address evidence demonstrating the *existence* of bad faith:

- (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
- (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
- (VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
- (VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties¹²³

122. *Id.*

123. *Id.*

The final factor — “the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this Section”¹²⁴ — merely incorporates the limited application of dilution into the determination of bad faith. This provides broader protection for marks that are “more” famous or “more” distinctive.

3. ICANN Arbitration and the UDRP

Shortly after the enactment of the ACPA, ICANN approved the Uniform Dispute Resolution Policy (UDRP),¹²⁵ an administrative regime applicable to certain domain name disputes, as well as the Rules governing the implementation and application of the policy (UDRP Rules).¹²⁶ The UDRP is incorporated by reference into all registration agreements entered into by ICANN-accredited registrars,¹²⁷ including those administering the .com, .org, and .net gTLDs (generic top-level domains), as well as many others.¹²⁸ Registration of a domain name utilizing any of these gTLDs thus places a limited contractual obligation on registrants to participate in ICANN’s UDRP administrative dispute-resolution procedures.¹²⁹

Remedies under the UDRP are limited to “the cancellation of [the registrant’s] domain name or the transfer of [the] domain name registration to the complainant.”¹³⁰ In many cases,¹³¹ however, these limited remedies are balanced by the expedited nature of the proceeding, the ease of

124. *Id.* § 1125(d)(1)(B)(i)(IX).

125. See UDRP Policy, *supra* note 11.

126. ICANN, Rules for Uniform Domain Name Dispute Resolution Policy [hereinafter UDRP Rules] (as adopted on Aug. 26, 1999 and approved by ICANN on Oct. 24, 1999), at <http://www.icann.org/dndr/udrp/uniform-rules.htm> (last visited Oct. 4, 2005).

127. ICANN FAQs, *supra* note 13.

128. *Id.*

129. *Id.*

130. UDRP Policy, *supra* note 11, ¶ 4(i). “Transfer is, by far, the most common remedy.” UDRP Opinion Guide: Berkman Center for Internet & Society, Harvard Law School [hereinafter UDRP Opinion Guide], Remedies, Topic 1.9.1 (Comment), at <http://cyber.law.harvard.edu/udrp/opinion/index.html>. See also *id.* (Reporter’s Notes) (citing WIPO/D2000-0019 for the proposition that UDRP panels lack “jurisdiction to order anything else than cancellation or transfer, even if law found applicable in accordance with Rule 15(a) provides for other remedies”).

131. As of June 15, 2003, more than 7,000 domain name disputes had been decided in the UDRP system, “compared with only a few hundred cases in national courts during that same period.” Laurence R. Helfer, *Whither the UDRP: Autonomous, Americanized, or Cosmopolitan?*, 12 CARDOZO J. INT’L & COMP. L. 493, 494-95 (2004). This disparity may be largely explained by the fact that the UDRP “system’s speed, low cost and automaticity have made it overwhelmingly popular with trademark owners — far more popular than litigation.” *Id.*

electronic filing,¹³² and the relatively minimal expense.¹³³ That said, proceedings under the UDRP do not prevent either party, registrant or complainant, from pursuing traditional litigation, as the UDRP expressly provides for submission “to a court of competent jurisdiction for independent resolution before [a UDRP] proceeding is commenced or after such a proceeding is concluded.”¹³⁴

Under Policy 4(a), a UDRP proceeding is triggered when a third-party Complainant alleges that: “(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;¹³⁵ and (ii) you have no rights or legitimate interests

132. See UDRP Opinion Guide, *supra* note 130, In-Person Hearings, § 1.7.9.1 (noting that under the UDRP “There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the Complaint”).

133. “The cost for filing a complaints and electing one arbitrator is \$1,500,” DuBoff & King, *supra* note 34, at 35, while “the cost of a three-member panel is \$4,000,” *id.* at 35 n.4. However, the cost may rise as the number of domain names at issue increases. *Id.*

134. UDRP Policy, *supra* note 11, ¶ 4(k). See also Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy, posted Oct. 25, 1999 [hereinafter ICANN Second Staff Report], available at <http://www.icann.org/udrp/udrp-second-staff-report-24oct99.htm> (last visited Oct. 4, 2005).

Except in cases involving “abusive registrations” made with bad-faith intent to profit commercially from others trademarks (e.g., cybersquatting and cyberpiracy), the adopted policy leaves the resolution of disputes to the courts . . . and calls for registrars not to disturb a registration until those courts decide. The adopted policy establishes a streamlined, inexpensive administrative dispute-resolution procedure intended only for the relatively narrow class of cases of “abusive registrations.” . . . [T]he policy’s administrative dispute-resolution procedure does not extend to cases where a registered domain name is subject to a legitimate dispute (and may ultimately be found to violate the challenger’s trademark). . . . The policy relegates all “legitimate.” disputes — such as those where both disputants had longstanding trademark rights in the name when it was registered as a domain name — to the courts; only cases of abusive registrations are intended to be subject to the streamlined administrative dispute-resolution procedure.

Id. ¶ 4.1(c). See also UDRP Opinion Guide, *supra* note 130, Effect of Court Proceeding, § 1.7.14.1(a) (stating that “In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the Complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.”).

135. UDRP Opinion Guide, *supra* note 130, Applicable Disputes, Topic 1.1.1(i)-(ii). “A complainant must have a trademark or service mark to bring a UDRP action. Domain name holders cannot initiate a UDRP action against a trademark owner.” *Id.* Topic 1.1.1 (Comment). “Registration of a domain name before a complainant acquires trademark rights in a name does not

prevent a finding of identity or confusing similarity . . . [h]owever it can be difficult to prove that the domain name was registered in bad faith as it is difficult to show that the domain name was registered with a future trademark in mind.” WIPO Overview of WIPO Panel Views on Selected UDRP Questions [hereinafter WIPO Overview], Question 1.4 (consensus view), *available at* <http://arbitrator.wipo.int/domains/search/overview/index.html> (last visited Oct. 4, 2005). *But see* UDRP Opinion Guide, *supra* note 130, Timing of Rights in the Mark, § 2.1.4.1 (The complainant must “have rights in a mark . . . before the disputed domain name is registered.”). “If the complainant owns a registered trademark then it satisfies the threshold requirement of having trademark rights.” WIPO Overview, *supra*, Question 1.1 (consensus view). *See also* UDRP Opinion Guide, *supra* note 130, Federally Registered Marks, § 2.1.1.1 (stating that “Federal registration of a mark is prime facie evidence of Complainant’s rights in the mark”). “The location of the registered trademark and the goods and/or services it is registered for are irrelevant when finding rights in a mark.” WIPO Overview, *supra*, Question 1.1 (consensus view). *See also* UDRP Opinion Guide, *supra* note 130, Foreign Registered Marks, § 2.1.1.2 (stating that “Foreign registrations of marks can establish a Complainant’s rights in a mark”). Generally, “[i]t is not the province of the UDRP to review the validity of [trademark] registrations issued by national governments.” *id.* Validity of Trademark Registration, Topic 1.4.5. However, “[i]n certain, highly limited circumstances, a panel may examine the circumstances of trademark registration to determine whether the registration satisfies UDRP requirements,” WIPO Overview, *supra*, Question 1.1. “Trademark registrations that are automatic or unexamined . . . may not always be owed the same deference as examined registrations.” *Id.* “Registration in the Supplemental Register is not sufficient,” although it may be if complainant “also show[s] secondary meaning.” UDRP Opinion Guide, *supra* note 130, Federally Registered Marks, § 2.1.1.1 (Reporter’s Notes) (citing WIPO/D2002-1103). *But see id.* (citing WIPO/DBIZ2002-0167 for the proposition that “Registration in the Supplemental Register might even prove that no rights existed at the time of registration”). In some cases, “State registration may establish Complainant’s rights in a mark, especially where the parties are from the same geographic area or where the mark has acquired secondary meaning beyond the original state.” *Id.* State Registered Marks, § 2.1.1.3. There is a split as to whether “[p]ending trademark or service mark applications can be used to help establish rights in a mark.” *Id.* Pending Applications, § 2.1.1.4. *See also id.* (Comments and Reporter’s Notes). Likewise, there is a split as to whether unregistered marks provide a basis for Complainant’s rights in a mark, where “[p]anelists from non-common law systems may require registration of the mark in order to establish rights in the mark.” UDRP Opinion Guide, *supra* note 130, Unregistered Marks, § 2.1.2.1 (Comments). Where the existence of common law trademark rights is considered, panels tend to focus on evidence demonstrating sufficient and continuous use of the mark in commerce, as well as secondary meaning. *See generally id.* Existence of Common Law Trademark, Topic 1.43, Establishing a Common Law Trademark, Topic 1.44, Unregistered Marks, § 2.1.2.1. Other evidence of a common law trademark includes:

- [1] Advertising, marketing, or promotional use of the alleged common law mark,
- [2] Third Party references to the alleged common law mark, [3] Widespread evidence of recognition among Internet users, [4] Sales of services under and by reference to the alleged common law mark, [and 5] Appropriate showing of prior continuous use in a given product and territorial market over a sufficiently long period of time.

Id. Establishing a Common Law Trademark, Topic 1.4.4; *see also* WIPO Overview, *supra*, Question 1.7 (consensus view). “Panels generally find rights in the names of well-known

in respect of the domain name; and (iii) your domain name has been registered and is being used¹³⁶ in bad faith.”¹³⁷

The UDRP requires that “the complainant must prove that each of [the] three elements” required under UDRP Policy 4(a) “are present,”¹³⁸ and must do so by a preponderance of the evidence.¹³⁹ However, the language and structure of Policy 4(c) has resulted in debate as to the proper evidentiary relationship between the complainant’s *prima facie* case under Policy 4(a)(ii) and the respondent’s rebuttal, particularly regarding shifting burdens of proof. If the complainant makes a *prima facie* showing as to Policy 4(a)(ii), then it is clear that the respondent must address the list of circumstances evidencing one’s rights to and legitimate interests in the domain name, as set forth in Policy 4(c).¹⁴⁰ The question concerns precisely what burden is shifting under this arrangement: “Some decisions

individuals and celebrities, based on having trademarked the name or through common law trademark protection.” UDRP Opinion Guide, *supra* note 130, Celebrity Names, § 2.1.2.2. *See also* WIPO Overview, *supra*, Question 1.6. Panels are less likely to transfer the domain where the domain is a personal name that is not well-known, absent evidence that the name was used commercially and had acquired secondary meaning.” UDRP Opinion Guide, *supra* note 130, Other Personal Names, § 2.1.2.3. *See also* WIPO Overview, *supra*, Question 1.6. “Panels are divided as to whether trade names qualify as a mark under 4(a)(i).” UDRP Opinion Guide, *supra* note 130, Trade Names, § 2.1.2.4. “A geographical name will satisfy 4(a)(i) if it is registered as a trademark and might satisfy 4(a)(i) if it performs functions similar to a registered trademark.” *Id.* Geographical Names, § 2.1.2.5. *See also* WIPO Overview, *supra*, Question 1.5 (consensus view) (citing as a consensus view that some geographical terms “can be protected under the UDRP, if the complainant has shown that it has rights in the term and that the term is being used as a trademark,” although “[n]ormally this would require the registration of the geographical term as a trademark”); *id.* (stating that “It is very difficult for the legal authority of a geographical area to show unregistered trademark rights in that geographical term on the basis of secondary meaning”). Certain panels have read 4(a)(i) to include “rights in Complainant’s domain name where the domain name functions as a common law trademark,” UDRP Opinion Guide, *supra* note 130, Complainant’s Domain Name, § 2.1.2.6; Patent Rights, § 2.1.2.7; Radio Call Letters, § 2.1.2.8.

136. “Within the element of bad faith, debate exists as to whether the domain must be registered and used in bad faith or whether either bad faith registration or bad faith use is sufficient.” UDRP Opinion Guide, *supra* note 130, Burden of Proof, § 1.3.1.1 (Comment).

137. UDRP Policy, *supra* note 11, ¶ 4(a)(iii); UDRP Opinion Guide, *supra* note 130, Applicable Disputes, Topic 1.1.1(iii).

138. UDRP Policy, *supra* note 11, ¶ 4(a); UDRP Opinion Guide, *supra* note 130, Burden of Proof, § 1.3.1.1.

139. UDRP Opinion Guide, *supra* note 130, Burden of Proof, § 1.3.1.1 (Comment). The preponderance standard requires “that a fact is proved when it is more likely than not that the fact is true.” *Id.* “The burden of proof is not satisfied by a mere showing of suspicion.” *Id.* (Reporter’s Notes) (citing WIPO/D2000-0067). *But see id.* (Reporter’s Notes) (citing WIPO/D2000-0847 for the proposition that “Generally, the appropriate standard in these proceedings is preponderance of the evidence; however in other jurisdictions other standards may apply.”).

140. *See id.* Burden Shifting, § 1.3.2.1 (Comments); *id.* Burden Shifting, § 4.1.2.1.

state that the burden of proof shifts while others maintain that it is not the burden of proof but rather the burden of production that shifts.”¹⁴¹ That debate may be dampened, however, by the World Intellectual Property Organization’s (WIPO)¹⁴² recent recognition of a consensus view that:

While the overall burden of proof rests with the complainant . . . a complainant is [merely] required to make out an initial *prima facie* case that the respondent lacks rights or legitimate interests. Once such *prima facie* case is made, respondent carries the burden of demonstrating rights or legitimate interests in the domain name. If the respondent fails to do so, a complainant is deemed to have satisfied paragraph 4(a)(ii) of the UDRP.¹⁴³

UDRP arbitrators are not required to apply a particular substantive law,¹⁴⁴ but simply to follow the Policy and associated UDRP rules.¹⁴⁵ Nor

141. *Id.* Burden Shifting, § 4.1.2.1 (Comment).

142. WIPO has been the dominant provider of UDRP service. See Jay P. Kesan & Andres A. Gallo, *The Market for Private Dispute Resolution Services — An Empirical Re-Assessment of ICANN-UDRP Performance*, 11 MICH. TELECOMM. & TECH L. REV. 285, 335 (2005). According to the statistics provided:

Between January 2000 and June 2003, the UDRP has evaluated 8,549 cases, and most of them have been divided among two main providers, NAF and WIPO.... WIPO and NAF have decided 95.5% of the cases. The closest competitor, with just 3.3%, eRes, is no longer a provider for the UDRP regime. *Id.* at 335.

Since the disappearance of eResolutions, WIPO and NAF have continued to divide up the market for UDRP resolution services. In 2003, “WIPO received 50% of the cases, NAF 46%, CPR 1.6% and ADNDRC 2%. At this time, the system seems to have reached equilibrium with two main providers receiving an almost similar quantity of cases.” *Id.* at 338.

143. WIPO Overview, *supra* note 135, Question 2.1 (consensus view).

144. See Holstein-Childress, *supra* note 31, at 580-81 (stating that “the UDRP itself neither requires panelists to apply the law of any particular nation, nor sets forth any choice of law guidelines for panelists”); *id.* at 581 (describing the UDRP as “conferring broad discretion upon panelists to apply a hodge-podge of governing law”); Hampton & McCue, *supra* note 31, at 21 (stating that “The arbitrators of UDRP disputes hail from all over the globe and bring widely differing understandings of substantive trademark law as well as procedural issues, such as burdens of proof”); *id.* (stating that “the arbitrators are not required to follow any particular substantive body of law in reaching their decisions or to view previous arbitration decisions as precedent”). But see DuBoff & King, *supra* note 34, at 35 (stating that “The substantive law applied by the arbitrator is determined by the contract between the registrar and the respondent”).

145. See Holstein-Childress, *supra* note 31, at 580-81 (stating that “the UDRP itself neither requires panelists to apply the law of any particular nation, nor sets forth any choice of law guidelines for panelists”); UDRP Opinion Guide, *supra* note 130, Applicable Law Under Rule 15(a), § 1.7.11.1 (stating that UDRP panels are to “decide a complaint on the basis of the statements

are the arbitrators bound by precedent,¹⁴⁶ although some measure of consistency is encouraged:

The UDRP does not operate on a strict doctrine of precedent. However panels consider it desirable that their decisions are consistent with prior panel decisions dealing with similar fact situations. This ensures that the UDRP system operates in a fair, effective and predictable manner for all parties.¹⁴⁷

This lack of binding (or even strongly influential) precedent, together with ambiguity regarding the substantive law to be applied in a particular case,¹⁴⁸ creates heightened uncertainty and a certain amount of reluctance on the part of some to utilize the UDRP.¹⁴⁹

These same factors also make it somewhat difficult to summarize the state of UDRP analysis and application. Thus, in the remainder of this section I will highlight those issues most relevant to the later discussion of trademark law and to show where consensus, such as it is, seems to be headed. This process is certainly aided by the recent release of the “2005 Overview of WIPO Panel Views on Selected UDRP Questions”¹⁵⁰ (WIPO 2005 Overview). However, WIPO continues to caution — as do many practitioners — that UDRP panels are not bound by this “informal overview” and “discussion.”¹⁵¹

and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable”).

146. See Hampton & McCue, *supra* note 31, at 21 (stating that “the arbitrators are not required to follow any particular substantive body of law in reaching their decisions or to view previous arbitration decisions as precedent”).

147. WIPO Overview, *supra* note 135, Question 4.1 (consensus view).

148. See Holstein-Childress, *supra* note 31, at 581 (footnotes omitted):

While some panelists apply the law of the country in which the parties are domiciled, others either merely apply the law of the panelists' country of origin or, more commonly, refuse to consider any nation state's law in favor of resolving the dispute exclusively in accordance with the UDRP rules.

149. See Hampton & McCue, *supra* note 31, at 21.

150. See WIPO Overview, *supra* note 135.

151. *Id.*

a. Confusing Similarity¹⁵²

According to the WIPO 2005 Overview, the “test for confusing similarity should be a comparison between the trademark and the domain name to determine the likelihood of confusion.”¹⁵³ As this statement suggests, the UDRP’s “identical or confusingly similar” standard appears to involve an “analysis of the same factors that govern a trademark infringement lawsuit’s finding of likelihood of confusion.”¹⁵⁴ However, there appears to have been some inconsistency in its application, particularly as to the relevance of web site content in the comparative analysis.¹⁵⁵ Nevertheless, the WIPO 2005 Overview asserts that a consensus has emerged adopting the view that the “content of a website (whether it is similar or different to the business of a trademark owner) is irrelevant in the finding of confusing similarity.”¹⁵⁶ the trademark and the domain name are simply all that matter. This view is premised on the notion of “initial interest confusion,” borrowed from trademark theory, “where a potential visitor does not immediately reach their site after typing a confusingly similar domain name, and is then exposed to offensive or commercial content.”¹⁵⁷ This suggests that content need not be commercial in nature to support the initial interest confusion rationale, but rather that “offensive” content is reason enough.

WIPO’s disregard for “offensive” content — often defined as that which is merely critical or derogatory of the trademark owner — is evidenced when the “identical or confusingly similar” analysis ignores web site content and focuses instead on a comparison between the trademark and the domain name. In the case of what are commonly known

152. This section does not address the issue of identity between the domain name and the complainant’s mark. The following general rules are noted, however: “A domain name will be considered identical even where Respondent deleted spaces between the words that form Complainant’s mark,” UDRP Opinion Guide, *supra* note 130, Spacing, § 2.2.1.1; “where Respondent merely added a gTLD to the Complainant’s mark,” *id.* TLDs, § 2.2.1.2; and “where Respondent merely added or deleted punctuation,” *Id.* Punctuation, § 2.2.1.3.

153. WIPO Overview, *supra* note 135, Question 1.2 (consensus view).

154. DuBoff & King, *supra* note 34, at 35.

155. *Cf.* UDRP Opinion Guide, *supra* note 130, Beyond Comparing the Mark and the Domain Name, § 2.2.3.1 (observing that “[s]ome panels look beyond the mark and the domain name when assessing confusing similarity, including the use of the mark on the website, the fame of the mark, whether Complainant and Respondent operated in similar lines of business, and other factors”), *with id.* § 2.2.3.1 (Comment) (stating that “a large number of Panels have held that any analysis beyond whether the actual mark and domain name are identical or confusingly similar is inappropriate”).

156. WIPO Overview, *supra* note 135, Question 1.2 (consensus view).

157. *Id.*

as “sucks” or “gripe” sites, the WIPO 2005 Overview reports the majority view that:

A domain name consisting of a trademark and a negative term is confusingly similar to the complainant’s mark. Confusing similarity has been found because the domain name contains a trademark and a dictionary word; or because the disputed domain name is highly similar to the trademark; or because the domain name may not be recognized as negative; or because the domain name may be viewed by non-fluent English language speakers, who may not recognize the negative connotations of the word that is attached to the trademark.¹⁵⁸

Only a minority of panels have disagreed and found that a “domain name consisting of a trademark and a negative term is not confusingly similar because Internet users are not likely to associate the trademark holder with a domain name consisting of the trademark and a negative term.”¹⁵⁹

Consistent with the apparent tendency towards a broad view of trademark rights, the majority of UDRP panels have generally found that what might be charitably characterized as *de minimus* differences between the domain name and the complainant’s mark are insufficient to overcome confusing similarity. This includes, for example: “Adding, deleting, or substituting letters or numbers”;¹⁶⁰ “reversing the words in Complainant’s mark”;¹⁶¹ or “Adding a word to Complainant’s mark.”¹⁶²

158. *Id.* Question 1.3.

159. *Id.*

160. UDRP Opinion Guide, *supra* note 130, Adding, Deleting, or Substituting Letters or Numbers, § 2.2.2.2.

161. *Id.* Reversing the Words in a Mark, § 2.2.2.3.

162. *Id.* Adding a Word to a Mark, § 2.2.2.4. One study has identified the following maxims: “Panels are even more likely to find confusing similarity where the word added relates to Complainant’s business,” *Id.* § 2.2.2.4 (Comment); “Adding an Internet related term will not preclude a finding of confusing similarity,” *Id.* Internet Related Term Added, § 2.2.2.5; “Addition of a geographical term will not preclude a finding of confusing similarity,” *Id.* Geographical Term Added, § 2.2.2.6; “Addition of a TLD will not preclude a finding of confusing similarity,” UDRP Opinion Guide, *supra* note 130, TLDs, § 2.2.2.7; “Changing the punctuation will not preclude a finding of confusing similarity,” *Id.* Punctuation, § 2.2.2.8; “Combining marks will not preclude a finding of confusing similarity,” *Id.* Combining Marks, § 2.2.2.9; and “Incorporating less than Complainant’s entire mark will not preclude a finding of confusing similarity,” *Id.* Incomplete or Abbreviated Marks, § 2.2.2.10. Other commentators have reported that a:

WIPO arbitration panel has . . . found confusing similarity in cases where the disputed domain name: Is phonetically identical or similar to complainant’s mark; Is a translation or transliteration of the famous mark; Gives an overall impression

b. Bad Faith

By its terms, UDRP Policy 4(a)(iii) is clearly conjunctive, requiring that the complainant prove both that the “domain name has been registered *and* is being used in bad faith.”¹⁶³ However, UDRP Policy 4(b), which provides a non-exhaustive¹⁶⁴ list of circumstances that “shall be evidence of the registration *and* use of a domain name in bad faith,”¹⁶⁵ is termed in the disjunctive:

- (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; *or*
- (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; *or*

of similarity to the famous mark; Merely adds a prefix to a famous mark; Combines a famous mark with a geographical term; or Is a combination of famous marks.

Hampton & McCue, *supra* note 31, at 22-23 (citations omitted).

163. UDRP Policy, *supra* note 11, ¶ 4(a)(iii).

164. *Id.* ¶ 4(b). The following have been identified as some of the factors

WIPO arbitration panels consider . . . to determine whether, in fact, the registration of a domain name was done in bad faith: Offer to sell, rent or license to complainant; Offer to sell, rent or license to general public; Offer to sell, rent or license for more than “out of pocket” costs; Pattern of conduct by respondent; Disruption of competitors business; Attracting internet users and then automatically hyperlinking to other sites, i.e. pornography or competitor’s sites; Giving of false contact information; Speculation in domain names; Inconceivable legitimate use; Prior knowledge or notice of the mark; Disclaimer; Prior relationship between parties; Acquiescence of mark owner; Cease and desist letters.

Hampton & McCue, *supra* note 31, at 24-25.

165. UDRP Policy, *supra* note 11, ¶ 4(b) (emphasis added).

- (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; *or*
- (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.¹⁶⁶

This construction has led to both debate and inconsistency in panel decisions, making resolution of this issue particularly vexing to practitioners.

ICANN's position at the outset seemed clear, as addressed by the ICANN Second Staff Report in 1999:

Several comments (submitted by INTA and various trademark owners) advocated various expansions to the scope of the definition of abusive registration. For example . . . These comments suggested that the definition should be expanded to include cases of either registration or use in bad faith, rather than both registration and use in bad faith While that argument appears to have merit on initial impression, it would involve a change in the policy adopted by the Board. The WIPO report, the DNSO recommendation, and the registrars-group recommendation all required both registration and use in bad faith before the streamlined procedure would be invoked. Staff recommends that this requirement not be changed without study and recommendation by the DNSO.¹⁶⁷

Nevertheless, panel opinions have been inconsistent. Some panels have required that the complainant prove just one of the four circumstances identified in UDRP Policy 4(b),¹⁶⁸ while other panels have required that

166. *Id.*

167. See ICANN Second Staff Report, *supra* note 134, § 4.5.

168. See UDRP Opinion Guide, *supra* note 130, The and/or Debate, § 3.1.1.2.1 (Comments).

[S]ome Panels will cite one or more of the registration related circumstances OR the use related circumstance, then claim that 4(a)(iii) is satisfied because 4(b) states that the circumstances are evidence of "of the registration and use of the domain name in bad faith." Instead of reading the language of 4(b) to mean that three of the circumstances listed are evidence of bad faith registration while one of the circumstances listed is evidence of bad faith use and therefore, a

the complainant prove at least one of the first three circumstances related to the act of registration *and* the fourth circumstance related to the use.¹⁶⁹ Despite the controversy, the 2005 WIPO Overview fails to address the issue and it remains somewhat unsettled.

As to what type of evidence may serve as the basis for a finding of bad faith, the WIPO 2005 Overview offers just two examples. The first is a consensus view that “[e]vidence of offers to sell the domain name in settlement discussions is admissible under the UDRP, and is often used to show bad faith,” primarily under UDRP Policy 4(b)(i).¹⁷⁰ The second is a

Complainant should prove at the least one of the first three circumstances PLUS the fourth circumstance, some Panels interpret 4(b) to mean that any one of the circumstances listed in 4(b) would, by itself, be sufficient for both bad faith registration and bad faith use.

Id. “[Other] Panels . . . have determined that, under certain circumstances, non-use or passive use of a domain may be evidence of bad faith. Thus . . . in effect, determin[ing] that bad faith registration alone is sufficient.” *Id.*

169. *See id.*

Those that interpret Policy Section 4(a) to require proof of both registration and use base their reasoning on statutory interpretation and general concepts of trademark law. They argue (a) the language of Section 4(a)(iii) language is clear despite the fact that the Section 4(c) examples are somewhat confusing; (b) the “legislative history” of the UDRP (Section 4.5 of the Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy) discusses the and/or debate and flatly rejects to change the “and” to an “or”; [c] Trademark law itself does not ordinarily find infringement in the absence of active commercial use as evidenced by the US Anti-cybersquatting Consumer Protection Act (15 USC 1125(d)(1)(A)(i) which specifically requires additional indication of a bad faith “intent to profit;” (d) trademark law does not grant a mark owner worldwide exclusive rights in a name nor should the UDRP. The UDRP should only be invoked when there is a specific intent to harm the mark owner (as all the bad faith examples indicate). Mere registration of a single domain name simply does not prove any of these elements.

Id.

170. WIPO Overview, *supra* note 135, Question 3.6. WIPO offers the following rationale for this position:

This is because many cybersquatters often wait until a trademark owner launches a complaint before asking for payment and because panels are competent to decide whether settlement discussions represent a good faith effort to compromise or a bad faith effort to extort. Also the legal criteria for showing bad faith directly specifies that an offer for sale can be evidence of bad faith.

Id.

consensus view that the circumstances as cited in UDRP Policy 4(b)(ii) — a pattern of conduct of preventing a trade or service mark owner from reflecting the mark in a corresponding domain name — can be evidenced by “a single case where the respondent has registered multiple domain names which are similar to known trademarks, [although] the registration of two domain names in the same case is not generally sufficient to show a pattern.”¹⁷¹

Some commentators have identified a more exhaustive list of what panels have considered as evidence of bad faith. Much of this evidence directly reflects the circumstances set forth in UDRP Policy 4(b), including the inference of bad faith from the registrant’s “non-use of the domain or . . . the absence of legitimate use,”¹⁷² or the registrant’s use of the domain “to link to other sites or . . . otherwise divert[] or redirect[] Internet traffic.”¹⁷³ Other evidence cited by commentators is less direct, such as the provision of false contact information;¹⁷⁴ respondent’s breach of contract or other agreement with complainant;¹⁷⁵ failure to perform a trademark search;¹⁷⁶ failure to respond to a cease-and-desist letter;¹⁷⁷ use

171. *Id.* Question 3.3.

172. UDRP Opinion Guide, *supra* note 130, Bad Faith Registration Inferred from Non-Use, § 3.1.1.3.11. It should be noted that “Panels have frequently determined that passive use satisfies the use requirement.” *Id.* Passive Use, § 3.1.2.1.

173. *Id.* Linking to Other Site, § 3.1.1.3.13. The UDRP Opinion Guide provides an analysis of what evidence has been used to satisfy the various provisions of UDRP Policy 4(b). *See id.* Circumstances Under Which an Intent to Sell may be Inferred, § 3.2.1.1.1, Circumstances Under Which an Intent to Sell was not Inferred, § 3.2.1.2.1 (listing evidence of an intent to sell under UDRP Policy 4(b)(i)); *Id.* Mark Owner is Prevented, §§ 3.2.2.1.1, 3.2.2.1.2, Pattern of Conduct, § 3.2.2.2.1 (listing evidence of preventing of a mark owner from reflecting his mark under UDRP Policy 4(b)(ii)); *Id.* § 3.2.2.2.2 (listing evidence of a pattern of conduct based on a scheme or plan to target under UDRP Policy 4(b)(iii)); UDRP Opinion Guide, *supra* note 130, Competitor/Competition § 3.2.3.1.1, Disruption, § 3.2.3.1.2 (listing evidence of disruption of a competitor’s business); *Id.* What Constitutes Use? § 3.2.4.1, What Constitutes Commercial Gain, § 3.2.4.2, What Constitutes a “Likelihood of Confusion”?, § 3.2.4.3, Circumstances Satisfying 4(b)(iv), § 3.2.4.4 (describing commercial use and listing evidence of an attempt to attract commercial gain by creating a likelihood of confusion). The UDRP Opinion Guide also provides an analysis of what evidence has been used to refute a claim of bad faith. *See id.* Respondent’s Domain Name, § 3.1.1.4.1, Use of Generic or Descriptive Term, § 3.1.1.4.2.

174. *Id.* False Contact Information, § 3.1.1.3.3.

175. *Id.* Breach of Contract or Agreement, § 3.1.1.3.4.

176. *Id.* Failure to Perform Trademark Search, § 3.1.1.3.6.

177. UDRP Opinion Guide, *supra* note 130, Failure to Respond to a Cease and Desist Letter or Other Communications, § 3.1.1.3.15.

of complainant's mark in metatags;¹⁷⁸ registration of a well-known mark;¹⁷⁹ registration of a misspelling or other variation of complainant's mark (typosquatting);¹⁸⁰ and even registration of a domain that is identical or confusingly similar to complainant's non-famous, not-well-known mark if the registrant knew of that mark.¹⁸¹

The WIPO 2005 Overview affirms many of these interpretations, albeit in a somewhat mitigated form, providing the following consensus view:

The lack of active use of the domain name does not as such prevent a finding of bad faith. The panel must examine all the circumstances of the case to determine whether respondent is acting in bad faith. Examples of circumstances that can indicate bad faith include complainant having a well-known trademark, no response to the complaint, concealment of identity and the impossibility of conceiving a good faith use of the domain name. Panels may draw inferences about whether the domain name was used in bad faith given the circumstances surrounding registration, and vice versa.¹⁸²

Other notable provisions of the WIPO 2005 Overview include a consensus view that "a disclaimer *cannot* cure bad faith,"¹⁸³ and a recognition that bad faith may be found in some cases where the domain name is registered before the trademark is even established.¹⁸⁴

178. *Id.* Use of Complainant's Mark in Metatags, § 3.1.1.3.16 (comments). "Panels occasionally find that the use of metatags falls under Paragraph 4(b)(iii) of the Policy (disruption of a competitor's business)." *Id.*

179. *Id.* Registration of Well-Known Mark, § 3.1.1.3.7.

180. *Id.* Typosquatting (Misspellings or Variations on a Mark), § 3.1.1.3.14.

181. *Id.* Registration of a Domain that is Identical or Confusingly Similar to a Mark Known to Respondent (That is not Necessarily Famous or Well-Known), § 3.1.1.3.9.

182. WIPO Overview, *supra* note 135, Question 3.2.

183. *Id.* Question 3.5. The following rationale and caveat are provided: "A disclaimer can also show that the respondent had prior knowledge of the complainant's trademark. However a disclaimer is sometimes found to support other factors indicating good faith or legitimate interest." *Id.*

184. *Id.* Question 3.1. The consensus view acknowledges that, "[n]ormally speaking, when a domain name is registered before a trademark right is established, the registration of the domain name was not in bad faith because the registrant could not have contemplated the complainant's non-existent right." *Id.* However, the following caveat is provided:

In certain situations, when the respondent is clearly aware of the complainant, and it is clear that the aim of the registration was to take advantage of the confusion between the domain name and any potential complainant rights, bad faith can be found. This often occurs after a merger between two companies, before the new

c. Rights and Legitimate Interests

Consistent with the structure of UDRP Policy 4(a), the complainant must make at least a *prima facie* showing that the registrant has “no rights or legitimate interests [in respect of the domain name].”¹⁸⁵ If the complainant is successful, then the burden shifts to the registrant to show one of three circumstances evidencing one’s rights to and legitimate interests in the domain name, as provided in UDRP Policy 4(c).¹⁸⁶

- (i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or
- (ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or
- (iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to

trademark rights can arise, or when the respondent is aware of the complainant’s potential rights, and registers the domain name to take advantage of any rights that may arise from the complainant’s enterprises.

Id.

185. *Id.* Question 2.2 (consensus view). It has been observed that “since it is difficult to prove a negative (i.e., that Respondent lacks any rights or legitimate interests in the mark) . . . a Complainant’s initial burden on this element is light.” UDRP Opinion Guide, *supra* note 130, What Must a Complainant Prove Under Paragraph 4(a)(ii), § 4.1.1.1 (Comments).

186. WIPO Overview, *supra* note 135, Question 2.2 (consensus view). At the extreme end, a registrant’s failure to show one of the four circumstances in UDRP Policy 4(c) may result in a finding that the registrant lacks a legitimate interest in the domain name, “even if it is a domain name comprised of generic word(s).” *Id.* The WIPO 2005 Overview describes the analysis in such a case as follows:

Factors a panel should look for when determining legitimate use would include the status and fame of the mark, whether the respondent has registered other generic names, and what the domain name is used for (a respondent is likely to have a right if it uses <apple.com> for a site for apples but not if the site is aimed at selling computers or pornography).

Id. “However: If a respondent is using a generic word to describe his product/business or to profit from the generic value of the word without intending to take advantage of complainant’s rights in that word, then it has a legitimate interest.” *Id.*

misleadingly divert consumers or to tarnish the trademark or service mark at issue.¹⁸⁷

However, UDRP Policy 4(c) has proven somewhat challenging for parties to UDRP proceedings, particularly those from the United States, as decisions under this requirement “have been less congruent with U.S. law.”¹⁸⁸ The most likely reason for this dissonance is that all three UDRP Policy 4(c) defenses invoke some analysis of “fair use,” a concept that varies from country to country,¹⁸⁹ and even within the United States.

III. SITUATING CYBERSQUATTING AMONG TRADEMARK PRINCIPLES

There is no question that the remedial structures and substantive regulations applied to cybersquatting are founded — historically, theoretically, and expressly — on the broad principles of trademark law. However, cybersquatting is still a distinct “wrong” occurring in a unique medium. Accordingly, the statutory and private arbitration regimes that have been created to address cybersquatting have modified both basic tenets and particular aspects of trademark law. However, altering these elements to resolve a specific problem conceptually linked to trademarks does not necessarily implicate identical rights and interests. This section of the Article seeks to situate cybersquatting rules and remedies among trademark principles, illuminating distinctions that, as I will discuss in Part IV, have in some degree expanded beyond the justifications upon which such distinctions were based, without adequate regard for foundational differences.

A. Toward Property: Theoretical Evolution in Trademark Law

The particulars of trademark law are certainly more than theoretical, but it is one area of law in which the theoretical battle has been uncommonly visible. Broadly speaking, one side of the debate conceives of trademarks as private property, with an expansive bundle of exclusive rights attendant to such ownership.¹⁹⁰ The other regards trademarks as an

187. UDRP Policy, *supra* note 11, ¶ 4(c).

188. Hampton & McCue, *supra* note 31, at 23.

189. *Id.* See also WIPO Overview, *supra* note 135, Questions 2.4, 2.5.

190. See, e.g., Simone A. Rose, *Will Atlas Shrug? Dilution Protection for “Famous” Trademarks: Anti-Competitive “Monopoly” or Earned “Property” Right?*, 47 FLA. L. REV. 653, 683-97 (1995) (making the argument that trademarks entail an earned property right). See also William M. Landes & Richard A. Posner, *The Economics of Trademark Law*, 78 TRADEMARK REP.

artificial monopoly in expression, to be avoided, constrained, or minimized.¹⁹¹ This argument is more than academic, as one's understanding of the rights and restrictions encompassed within trademark protections may be strongly influenced by the theoretical principles to which one ascribes. Not surprisingly, the development of trademarks, and the legal protection afforded to them, embodies a certain ebb-and-flow between these viewpoints.

Modern trademark protections are rooted in the common law tort of deception through misrepresentation as to the source of goods, and thus their content, quality, warranty, etc.¹⁹² Consistent with this action, common law trademark rights are premised on use in commerce and a particular conception of reputation.¹⁹³ The mark serves both as an indicator of source¹⁹⁴ and as shorthand for all of the information that consumers might read into that identification, such as quality, utility, mode of manufacture, and the like.¹⁹⁵ Thus, the mark, when sufficiently unique, embodies the producer's reputation and, where customers are happy, the goodwill that the producer's reputation has created. This, in turn, gives value to the mark, protecting both producers from diversion of trade and consumers from receiving a lesser good or service than expected.

Common law trademark rights are, as a practical matter, limited geographically. Such a mark carries trademark significance only in the geographic area in which consumers recognize it as an indication of source. Indeed, for many early marks, geographic identification was an integral part of the information conveyed by the trademark. Accordingly, identical or similar marks could co-exist in distinct geographic markets without undermining their trademark significance.

As trademark law progressed towards a federal system of rights recognition, the debate over its theoretical bases accelerated. Proponents of expansive trademark protections urged a full embrace of the private

267 (1988) (providing an economic analysis and justification for the recognition of property-like trademark rights).

191. See, e.g., Daniel M. McClure, *Trademarks and Unfair Competition: A Critical History of Legal Thought*, 69 TRADEMARK REP. 305, 306 (1979) (describing the monopoly view of trademarks); Rose, *supra* note 190, at 664-73 (providing a skeptic's overview of intellectual property rights, including trademark rights, as anti-competitive monopolies).

192. McClure, *supra* note 191, at 314-16 (describing the early development of trademark law in America).

193. Landes & Posner, *supra* note 190, at 272, 279-80.

194. Rose, *supra* note 190, at 658 (describing a process by which trademarks "become source identifiers").

195. *Id.* (arguing that trademarks also serve as "indicators of quality assurance and advertising power").

property conception, replete with all of the positive imagery that such an idealized vision evokes — the incentive to create, natural rights in the fruit of one's labor, and the social utility of highest and best use.¹⁹⁶ Critics, on the other hand, continued to press the concept of trademarks as a monopoly, and thus an evil to be tolerated only to the extent necessary to serve a specific set of social benefits related to consumer protection and economic efficiency.¹⁹⁷ In the end, it seemed that under the fairly narrow terms of the Lanham Act the monopoly view had largely, if not entirely, prevailed. However, the act instead proved to be a useful baseline against which to leverage future movement toward a property conception.

Indeed, since the passage of the Lanham Act, legal institutions have methodically expanded the boundaries of trademark protections. We have seen a broadening not only in the scope of protectable trademark subject matter, but also in the private rights incumbent in that protection. Not surprisingly, this expansion has met with some resistance. But the vagaries of common law and statutory language, and the particularly complex interplay between these authorities as they exist in trademark law, have proven amply flexible to accommodate reinterpretation. With the theoretical foundations of trademark protection (whether monopoly- or property-based) seemingly unmoored, the substantive boundaries of that protection have tended to expand from the relatively narrow grant embodied in the Lanham Act to more substantial rights paralleling those associated with traditional private property. Indeed, it can be persuasively argued that our legal institutions now generally embrace a view of trademark protection in which the bundle of rights held by the trademark proprietor is so broad as to nearly evoke Blackstone's traditional view of the real property owner.

This expansion, justified within the traditional likelihood-of-confusion framework, is well documented, and need not be reviewed in great detail. The first area of expansion has been in the area of subject matter. Seizing on a broad statutory definition of a trademark that includes any "device,"¹⁹⁸ courts have moved well beyond words and pedestrian symbols to discern a broad universe of things that can qualify as a trademark — including slogans, trade dress, shape, color, design, and configuration. A second area of expansion has been the broadening of infringement beyond the deception-based fraud of passing off one's own goods or services for those of another, where the harm is primarily to the consumer, to include free-riding on the goodwill of another, where the harm is primarily to the

196. See generally Rose, *supra* note 190, at 672.

197. See generally McClure, *supra* note 191, at 306.

198. See 15 U.S.C. § 1127 (2000).

trademark holder. A third area of expansion has been to extend the trademark holder's rights to include protection not just from goods or services that are directly competitive, but also from goods or services that are closely related to those of the trademark holder. A fourth area of expansion (and this list is certainly not exhaustive) has been to broaden the concept of what "confusion" trademark protections are intended to avoid. Rather than limiting protection to instances of confusion over source, courts have found infringement where the confusion is said to implicate sponsorship, endorsement, or affiliation. The concept has been further expanded by the recognition by many Circuits of the doctrine of "initial interest confusion."¹⁹⁹ This doctrine allows a trademark holder to stop competitors from attracting a consumer's attention by use of another's trademark, even where there is no likelihood of confusion; i.e., any confusion would be cleared up quickly, prior to purchase.

Each of these new areas of protection — each new stick in the bundle of trademark rights — pushes trademarks closer to our conception of private property. As the number of uses from which the trademark holder may exclude all others grows, we arguably approach an image of exclusive dominion. As we provide greater protections against private harm rather than to promote the public benefit, we move away from expressive monopoly concerns and toward property rights. Furthermore, as source confusion is eclipsed by the trademark holder's right to remedy any possible confusion as to the existence of any connection between the trademark owner and the goods, services, or expressive acts of another, we seem ready to jettison the idea of a limited monopoly altogether.

With the addition of the federal dilution statute in § 43(c) of the Lanham Act,²⁰⁰ the movement toward property rights has taken a tremendous leap forward, at least for a few chosen marks. Section 43(c) codified the extension of trademark rights (in the case of "famous" and "distinctive" marks) beyond mere protection against customer confusion to the reputation of the mark itself. Accordingly, dilution has been described as "the gradual 'whittling away' of a trademark's value,"²⁰¹ usually in one of two forms: blurring or tarnishment.²⁰² Furthermore, a

199. See, e.g., *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036 (9th Cir. 1999).

200. 15 U.S.C. § 1125(c) (1999).

201. *Playboy Enters., Inc. v. Welles*, 279 F.3d 796, 805 (9th Cir. 2002) (citations omitted).

202. *Id.* But see *Moseley v. V Secret Catalogue, Inc.*, 537 U.S. 418, 432 (2003) (raising the question of whether blurring and tarnishment are truly embraced by the FTDA, but without addressing it).

§ 43(c) claim does not require that the plaintiff show competition between the goods or services in question.²⁰³ Nor must the plaintiff show a likelihood of confusion, mistake, or deception.²⁰⁴

As a result, § 43(c) expressly extends trademark protections beyond the narrow confines of source confusion; unjustified by a reduction in search costs, informational efficiency, or related economic considerations. The Supreme Court itself has recognized that “[u]nlike traditional infringement law, the prohibitions against trademark dilution are not . . . motivated by an interest in protecting consumers.”²⁰⁵ Indeed, dilution expressly frees trademarks from the quid pro quo implicit in the monopoly-based theory of the original Lanham Act. In so doing, § 43(c) seems to at least approach property-like trademark rights in gross. This solidifies the argument that trademark rights are no longer entirely confined by the monopoly rationale, if they ever were, but should instead be read broadly to embrace the romantic vision of economic efficiency, progress, and just rewards embodied in private property.

This is not to say that these rights are unlimited. In addition to those constraints apparent in the terms of the infringement and/or dilution statutes — likelihood of confusion, commercial use, fame and distinctiveness, bad faith, etc. — the Lanham Act incorporates an express statutory grant of fair use. Moreover, the act is subject to limitations of constitutional fair use. These restrictions are integral to the balance between private and public rights in expression. Certainly, recent developments in trademark law have appropriated specific, additional rights from the public and allocated them to private interests but these encroachments have not yet eviscerated many of the most important limitations.

Blurring involves a diminution in the uniqueness or individuality of a mark because of its use on unrelated goods. Tarnishing occurs when a trademark is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context, with the result that the public will associate the lack of quality or lack of prestige in the defendant’s goods with the plaintiff’s unrelated goods.

Scott Fetzer Co. v. House of Vacuums, Inc., 381 F.3d 477, 489 (5th Cir. 2004) (internal quotes and citations omitted).

203. See *Moseley*, 537 U.S. at 429.

204. *Id.*

205. *Id.* at 429. See also Holstein-Childress, *supra* note 31, at 576 (noting that the federal dilution statutes embody a “shift to a property-based trademark protection regime that primarily values the marketing function of trademarks — free of any constraint posed by the consumer confusion-based theories”).

B. Cybersquatting as a Point of Expansion

Trademark law has clearly evolved towards an expansive, property-like conception of exclusive rights. Yet even this broad protection seemed insufficient to solve the particular problem of cybersquatting. As such, the remedial systems developed to address cybersquatting imbued trademark holders with the additional rights they needed to secure their interests in domain names. Many of these changes chaff under our traditional view of trademarks, but have been largely excused as a narrow, if somewhat drastic, response to a specific and intentional wrong. The question seems to be whether these expansions now exceed their supporting rationales.

1. Expansion within the Substantive Terms of the ACPA

The ACPA expands the trademark holder's rights in significant ways. It mirrors and in some cases moves beyond the additional protections provided in the federal dilution statute (§ 43(c) of the Lanham Act), and closer to an exclusive property rights conception in the context of domain names. As with § 43(c), the ACPA applies without regard to the goods or services of the parties.²⁰⁶ Unlike § 43(c), however, the ACPA is not limited to marks that are both famous and distinctive,²⁰⁷ but applies to a much broader universe of marks that are either famous or distinctive. The ACPA also eliminates²⁰⁸ the use-in-commerce and commercial-use requirements of § 43(c).²⁰⁹ Finally, the ACPA redirects the substantive inquiry from the issue of the mark's capacity to identify and distinguish goods and services,²¹⁰ to a showing of mark identity (i.e., identical or confusingly similar)²¹¹ plus bad faith.²¹² This effectively narrows the multi-factored confusion standard to two primary inquiries, thus broadening the trademark holder's rights. This expansion is reflected in Congress's express recognition of the need for protection extending beyond diversion of trade by a competitor, to the protection of a company's goodwill from even the slightest injury, separate and apart from any concern over consumer protection.²¹³

206. 15 U.S.C. § 1125(d)(1)(A) (1999).

207. See 15 U.S.C. § 1127(c)(1) (2000) (regarding application of the federal dilution statute only to marks that are famous *and* distinctive).

208. 15 U.S.C. § 1125(d)(1)(A)(ii)(I), (II).

209. See *generally id.* § 1125(d).

210. See *Moseley*, 537 U.S. at 433.

211. 15 U.S.C. § 1125(d)(1)(A)(ii)(I), (II).

212. *Id.* § 1125(d)(1)(A)(i).

213. See *id.* § 1125(d)(1)(A)(ii)(V); *supra* Part II(C)(2)(a) (addressing conceptions of cybersquatting).

The ACPA factors for evidence of bad faith, which center on the intent of financial gain,²¹⁴ together with the elimination of the use-in-commerce and commercial-use requirements,²¹⁵ would certainly rile Internet exceptionalists.²¹⁶ Their speculation and foresight would now be labeled as trespass; their claims of a new territory apart from existing off-line power structures, rights, and obligations, would be rejected. Nevertheless, if this is where we left it, that result might at least be defensible in terms of trademark law. The ACPA was seen as a rational and targeted response to a perceived wrong narrowly tailored to resolve that problem through the protection of established interests in a new but familiar medium (and not a newly created, self-governing territory), informed by existing principles and analogous precedent, subject to procedural due process, and limited by both statutory and constitutional concepts of fair use. As such, the ACPA's approach to domain name rights and dispute resolution might well have settled comfortably into the landscape of trademark law, but the UDRP is an entirely different story.

2. Expansion within the Substantive Terms of the UDRP

For purposes of this analysis, it is necessary to note that the UDRP differs substantively from the ACPA in at least three important areas in addition to the vastly expanded rights already conferred under the federal dilution statute and the ACPA.²¹⁷ The first relates to the standard of bad faith and the way in which it is applied. The second relates to the relationship between the bad faith standard and the defenses of noncommercial and fair use, and particularly the availability of those defenses where there exists an intent for commercial gain or to tarnish the mark of another. This point also implicates the ACPA's distinct limitation on when one's intent for commercial gain or tarnishment may be considered, and the absence of such limitation in the UDRP. The third involves the presence of an express safe-harbor provision for "innocent" actors.

The ACPA focuses on a registrant's bad faith intent to profit.²¹⁸ In determining whether that standard has been met, the ACPA provides a list of nine non-mandatory, non-exhaustive factors to be considered.²¹⁹ These factors expressly balance the registrant's bona fide interest in the domain

214. *See supra* Part II(C)(2)(b) (addressing bad faith).

215. *See* 15 U.S.C. § 1125(d).

216. *See supra* Part I.

217. *See supra* Parts II(C)(1)-(2), III(A), III(B)(1).

218. *See* 15 U.S.C. § 1125(d)(1)(A)(i); *supra* Part II(C)(2)(b).

219. *See supra* Part II(C)(1)(b) (discussing bad faith).

name, both commercial and noncommercial,²²⁰ with evidence of bad faith intent to profit or otherwise harm the trademark holder.²²¹ In contrast, the UDRP avoids any type of balancing test, instead providing four independent bases for a finding of bad faith.²²² Any one of these bases, standing alone, may be sufficient to satisfy UDRP Policy 4(c).²²³ If the complainant is successful in establishing a *prima facie* case on any one of these bases, the burden shifts to the registrant to prove that he has rights to and a legitimate interest in the domain name.²²⁴ The ACPA's balancing approach is more consistent with American trademark law,²²⁵ while the UDRP clearly shifts the balance of rights toward the trademark holder.

As part of the ACPA's balancing approach to bad faith, § 43(d) indicates that the court should consider, *inter alia*, the registrant's "bona fide noncommercial or fair use of the mark in a site accessible under the domain name"²²⁶ in determining whether such bad faith exists. This factor stands alone as one of the nine to be considered in making a determination as to bad faith, with no qualification of its applicability. Similarly, the UDRP allows the registrant to demonstrate his rights or interests in the domain name by showing that he is "making a legitimate noncommercial or fair use of the domain name."²²⁷ However, the UDRP places a significant qualifier on this defense by linking it to evidence of bad faith. Under the UDRP, such use must be made "without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue."²²⁸ Examining the four circumstances evidencing bad faith under the terms of the UDRP,²²⁹ it becomes clear that this qualifier all but swallows the defense.

This distinction is even more pronounced when one considers the limitation the ACPA places on a court's consideration of the registrant's intent for commercial gain or to tarnish. The ACPA provides that evidence of bad faith may include the registrant's

220. See generally *id.*; 15 U.S.C. § 1125(d)(1)(A)(i); *supra* Part II(C)(2)(b).

221. See *supra* Part II(C)(1)(b); 15 U.S.C. § 1125(d)(1)(B)(i).

222. See *supra* Part II(C)(3); UDRP Policy, *supra* note 11, ¶ 4(b).

223. See *supra* Part II(C)(3) (discussing controversy over the interpretation of UDRP Policy 4(c)).

224. See *supra* Part II(C)(2)(a) (discussing controversy regarding shifting burdens of proof under the UDRP Policy).

225. See generally *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492 (2d Cir. 1981); *AMF, Inc. v. Sleekcraft Boats*, 579 F.2d 341 (9th Cir. 1979).

226. 15 U.S.C. § 1125(d)(1)(B)(i)(IV) (1999).

227. UDRP Policy, *supra* note 11, ¶ 4(c)(iii).

228. *Id.*

229. *Id.* ¶ 4(b).

intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, *by creating a likelihood of confusion* as to the source, sponsorship, affiliation, or endorsement of the site. . . .²³⁰

Thus, absent this connection between the registrant's bad intent and the creation of a genuine likelihood of confusion, this factor should not be considered. The UDRP contains no such limitation,²³¹ further broadening the impact of its qualification on the registrant's noncommercial or fair use defense and effectively expanding the rights of the trademark holder once again.

Given the UDRP's one-strike approach to bad faith and significant limitations on the noncommercial or fair use defenses, one might expect the UDRP to provide an express, independent safe-harbor provision for "innocent" actors outside the intended reach of an anti-cybersquatting regime. However, no such provision is provided. The ACPA, by comparison, provides that the "[b]ad faith intent described under subparagraph (A) *shall not* be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful."²³² Thus, in addition to providing a balancing approach more akin to American trademark law, as well as an unqualified consideration of a registrant's noncommercial or fair use, the ACPA also provides a safe harbor for "innocent" registrants, focusing the applicability of ACPA narrowly on the most egregious cases of bad intent.

Finally, the UDRP's radical expansion of the trademark holder's substantive rights in domain names is further exacerbated by the extension of these rights to almost any mark. As discussed above, the expanded protections of the federal dilution statute are limited to marks that are both famous and distinctive,²³³ while the even broader protections of the ACPA are limited to marks that are either famous or distinctive.²³⁴ The UDRP, on the other hand, applies without regard to the strength of the mark.²³⁵ Thus,

230. 15 U.S.C. § 1125(d)(1)(B)(i)(V) (emphasis added).

231. UDRP Policy, *supra* note 11, ¶ 4(c)(iii).

232. 15 U.S.C. § 1125(d)(1)(B)(ii) (emphasis added).

233. *Id.* § 1125(c)(1).

234. *Id.* § 1125(d)(1)(A).

235. UDRP Policy, *supra* note 11, ¶ 4(a).

all marks — famous or not, distinctive or not — are provided with the “tarnishment” exception to the noncommercial and fair use defenses.²³⁶

3. Systemic Expansion Beyond Substantive Terms

The extension of trademark rights under the UDRP is further amplified when the Policy’s substantive expansions are leveraged against procedural and institutional biases in favor of the trademark holder. On the procedural side, the UDRP imposes unreasonable time limits, provides no real opportunity for appeal, and fails to sanction over-aggressive enforcement actions undertaken by trademark holders to intimidate registrants. Moreover, the process lacks transparency and provides little in the way of clear principles or standards to govern decisions. There is also a credible institutional argument that the UDRP system is set up, and the service providers selected, so that it favors trademark holders. Indeed, the numbers appear to demonstrate this.

Procedural biases are apparent from the outset of a UDRP action. The complainant trademark holder has nearly unlimited time to prepare her case before the filing of a UDRP complaint. In contrast, the registrant has just twenty days to prepare his response.²³⁷ Furthermore, these are generally the only documents considered by the panel, although the parties may request supplemental filings.²³⁸ Hearings are extremely rare.²³⁹ In most cases, the panel is given just fourteen days to reach its decision.²⁴⁰ Following that decision (which, as discussed below, is most likely to go against the registrant), the losing party has just ten days to seek relief from a court of competent jurisdiction before the panel’s decision to cancel or transfer the domain name takes effect.²⁴¹ In all, the entire process can take just a few weeks; barely enough time for a registrant to seek legal assistance, much less produce an adequate defense. Moreover, there is little or no penalty under the UDRP for the over-aggressive use of UDRP processes to gain control of domain names from legitimate owners, a ploy

236. See *supra* Part II(C)(3)(b).

237. UDRP Rules, *supra* note 126, § 5(a); See also *id.* § 5(d) (providing, in part, that “At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response.”).

238. *Id.* § 12 (providing that “In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.”).

239. *Id.* § 13 (providing that “There shall be no in-person hearings . . . unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint”).

240. *Id.* § 15(b).

241. UDRP Policy, *supra* note 11, ¶ 4(k).

known as “reverse domain name hijacking,” even in clear cases of bad faith. Finally, there is no real opportunity for appeal, other than through a time-consuming and expensive court proceeding filed within the ten-day period provided for under the UDRP.

The available evidence also suggests that an institutional bias in favor of trademark holders may also exist. Procedurally, the UDRP places the choice of provider in the hands of the complainant,²⁴² who, by definition, holds the rights to a trademark that is allegedly identical or confusingly similar to the domain name in question.²⁴³ Approved UDRP providers are thus competing against one another for the provision of services to trademark holders, many of whom own the rights to multiple trademarks and will therefore likely require future services. This economic reality creates a strong incentive for UDRP providers to render decisions that favor trademark holders. Not surprisingly, the two dominant UDRP providers, WIPO and the National Arbitration Forum (NAF), are both seen as favoring strong intellectual property rights.

Available statistics regarding the outcome of UDRP proceedings support this view. As of May 2004, over eighty percent of the nearly eight thousand proceedings disposed of by decision had favored the complainant, resulting in cancellation or transfer to the trademark holder.²⁴⁴ Less than twenty percent of the proceedings had resulted in a decision for the registrant.²⁴⁵ The remaining one percent had resulted in a split decision.²⁴⁶ Broken down by the number of domain names at issue, rather than the overall proceeding, these numbers favor the trademark holders to an even greater extent. Of the more than thirteen thousand domain names at issue, eighty-one percent were cancelled or transferred to the trademark holder.²⁴⁷ Approximately fourteen percent were retained by the registrant.²⁴⁸ The remaining five percent were split decisions.²⁴⁹ It is telling that complainants were significantly more successful in UDRP

242. *Id.* ¶ 4(d); *id.* ¶ 3.

243. *Id.* ¶ 4(a)(i).

244. ICANN Statistical Summary of Proceedings Under Uniform Domain Name Dispute Resolution Policy, as of May 10, 2004, [hereinafter ICANN Statistical Summary] at <http://www.icann.org/udrp/proceedings-stat.htm> (last visited Oct. 4, 2005) (indicating 6262 out of 7790 decisions, or 80.4%).

245. *Id.* (indicating 1468 out of 7790 decisions, or 18.8%).

246. *Id.* (indicating 60 out of 7790 decisions, or 0.8%).

247. *Id.* (indicating 10,719 out of 13,311 domain names, or 81.5%).

248. *Id.* (indicating 1,892 out of 13,311 domain names, or 14.2%).

249. ICANN Statistical Summary, *supra* note 244 (indicating 640 out of 13311 domain names, or 4.8%).

actions undertaken by eResolutions, the third most popular provider, and eResolutions is now out of business.²⁵⁰

IV. BEYOND PROPERTY? LOSING TOUCH WITH LIMITING PRINCIPLES

The issues coming out of this expansion of trademark holder rights in the context of domain name disputes are whether and to what extent these additional rights can be squared with the foundational principles upon which they were constructed. That foundation rests upon two pillars. The first is a product of practical concerns and competing interests which were found to justify the alteration of certain tenets of trademark protection for the purpose of addressing the very specific and perceptually grave harm of cybersquatting. The second is composed of theoretical justifications for the expansion of trademark protections toward a private property-like conception of broad exclusive rights, but limited by basic constitutional interests.

In this final section of this Article, I will argue that the UDRP dispute resolution system has lost touch with the basic principles which support it. The UDRP was intended to strike a bargain, sacrificing certain due process protections in favor of efficiency, speed, and reduced costs. Because of this, the UDRP was in theory to be sharply limited, applicable only to the most obvious and egregious cases of bad faith and abusive domain name registration. In substance and practice, however, UDRP panels have in essence grossly exceeded their intended jurisdiction. The result is a dramatic shift in favor of the trademark holder, creating through seizure and reallocation some sort of absolute right beyond property. Not only have protections outstripped the rationales of consumer protection and preservation of goodwill, they have arguably invaded constitutional interests.

A. *Beyond Cybersquatting Exceptionalism*

The ACPA provides a useful baseline, as it is intended to apply to a fairly broad but defensible conception of cybersquatting.²⁵¹ Included in this conception is what might be referred to as “classic” cybersquatting, in which the registrant intends to profit monetarily through arbitrage (or blackmail) by selling the domain name to the highest bidder, whether that be the owner of an identical or similar trademark, or his competitor.²⁵²

250. See Kesan & Gallo, *supra* note 142, at 335.

251. See *supra* Part II(C)(2)(a).

252. S. REP. NO. 106-140, at 9 (1999).

Another form of cybersquatting seeks to deceive consumers in such a way that they purchase counterfeit goods thinking that they are the real thing.²⁵³ A third form of cybersquatting involves the registration of domain names identical or similar to well-known marks, leveraging consumer confusion and free-riding on the mark's goodwill so as to divert traffic or trade.²⁵⁴ In essence, the ACPA defines cybersquatting by the egregiousness of the registrant's conduct and objective, focusing on his bad faith intent to profit through commercial gain.

On its face, as it defines "bad faith," the UDRP at first appears consistent with this rather limited universe of circumstances.²⁵⁵ However, expansive interpretation by UDRP panels has stretched its application far beyond any recognizable conception of intentional, greed driven, bad faith cybersquatting. UDRP panels have found evidence of bad faith in, *inter alia*, non-use or the absence of legitimate use, the provision of anonymous or false contact information, the failure to perform a trademark search, or the mere registration of a well-known mark.²⁵⁶ Such evidence simply cannot be matched to any of the offensive conduct that anti-cybersquatting regimes seek to remedy and deter.

This expansion of the bad-faith concept might itself have a nominal impact if the UDRP provided for and effectively applied a sufficiently robust counterbalance. Unfortunately, the availability of a noncommercial or fair-use defense has been minimized, particularly by its qualification where tarnishment is found and the failure to require likelihood of confusion as a prerequisite for tarnishment. Not only does this fail to provide an adequate balance to bad faith; it effectively broadens the conception of cybersquatting even further. Likewise, the absence of an express safe harbor provision for innocent actors is particularly telling, given the regime's intended focus on egregious conduct.

The impact of this overbreadth is not limited to mere labels. Both the ACPA and, to an even greater extent, the UDRP were intended to broaden the trademark holder's rights, starting with the federal dilution statute as a baseline and expanding certain aspects of protection to address a specific problem. Outside the strict confines of cybersquatting, those expanded rights simply do not make sense.

Trademark protections have been traditionally rationalized on the basis of consumer protection and economic efficiency.²⁵⁷ These rationales

253. *See id.*

254. *See id.*

255. *See supra* Part II(C)(3)(b).

256. *See supra* text accompanying notes 174-81.

257. *See supra* Part III(A).

extend from the trademark's function as an indication of source, sponsorship, endorsement, or affiliation. Their premise is that through experience with the product or service, consumers instill the trademark with information about its content, quality, utility, etc., even if the product or service is not identical to that with which the consumer has previous experience. This communication of desirable but obscure information is what creates economic efficiencies through, among other things, the reduction of search costs. It also benefits consumers by motivating trademark holders to maintain and improve quality of their goods and services. Trademark holders are in turn benefited by the trademark's protection against diversion of trade. More recently, expanded trademark protections have been premised on the maintenance of goodwill, independent of any customer confusion. This implicates several private interests, including protection of the mark against tarnishment or blurring and punishment of improper free-riding. Implicit in these private interests, however, is the perceived public benefit that flows from the incentive to invest in one's reputation.

The current application of the UDRP cannot be justified under even the most expansive view of trademark rights. There is no rationale, for instance, for the extension of dilution-based rights to trademarks that are neither famous nor distinctive. And there is certainly no rationale for limiting the noncommercial and fair use defenses because of the tarnishment of these pedestrian marks.

B. In Derogation of Constitutional Interests and the Rule of Law

The UDRP requires us to sacrifice quite a bit in exchange for efficiency, speed, and ease. This bargain may have made sense when narrowly tailored to a specific and serious problem, but in light of the UDRP's expansion into more benign instances of domain name conflict, that bargain needs to be reexamined. Due process concerns and notions of fairness require transparency, consistency, and equal treatment. The rule of law requires a measure of certainty such that one can be guided in his actions and secure in his rights and obligations. As it is now interpreted and applied, the UDRP dispute resolution policy fails to meet these standards.

All domain name registrants are bound to the UDRP system. UDRP panels are not required to apply a particular substantive law, nor are they bound by precedent. There is little transparency and great uncertainty. Moreover, the system is rife with procedural and institutional biases favoring trademark holders. There is little opportunity for defense of one's position and the practical ability for a meaningful appeal is limited. There

is no sanction for actions brought in bad faith. In all, domain name registrants are at the mercy of a system created to benefit trademark holders not only as a matter of systemic efficiency but in result as well.

V. CONCLUSION

Any newcomers to the process of domain name dispute resolution as well as general practitioners are likely a bit shocked at what they have read. Arbitration-based systems like the UDRP are touted as efficient, fast, and fair. But to whom? Both as a matter of substance and procedure, the UDRP expands trademark-holder rights even beyond the broad property-like rights emerging under U.S. trademark law. These expansions have been reinforced by institutional biases in favor of trademark holders. As a result, cybersquatting protections have exceeded the very rationale of exceptionalism justifying their creation. The bargain at the heart of these policies — premised on a narrow application to the most obvious and egregious cases of bad faith — is no longer supported. As such, the validity of the UDRP as it is now applied is in doubt.

